GENERAL DYNAMICS

Sectéra® and *Talk*SECURE™ PSTN Connect vIPer™ Phone User’s Guide

Table of Contents

Table of Figures

Table of Tables

1 Welcome

Congratulations on your purchase of PSTN Connect for your vIPer Phone. This guide will familiarize you with the capabilities of your vIPer Phone when used with the PSTN Connect accessory. If you are a Sectéra vIPer user, you should also read the *Sectéra vIPer Phone Supplement*.

NOTE to Sectéra vIPer Phone users: The Sectéra vIPer Phone is a Controlled Cryptographic Item (CCI). It is classified to the level of the key when filled with Type 1 key and the PIN is entered. It is CCI when locked or zeroized. Refer to your COMSEC custodian for handling and shipping instructions.

The vIPer Phones provide secure telephony using the latest Secure Communications Interoperability Protocol (SCIP) signaling[1]. In addition, the vIPer Phones provide clear voice using standard protocols defined by governmental and regulatory agencies. They have been tested for interoperability on a wide variety of networks and with various equipment configurations.

If you purchased your vIPer Phone with the PSTN Connect accessory, the phone will already be loaded with the PSTN Connect software. If you purchased the PSTN Connect accessory separately, you will need to install the PSTN Connect software from the supplied CD on your vIPer Phone before use. See Sections 6 and 7 for more information.

The *Talk*SECURE vIPer Phone provides encryption using Universal Cert (UnivCert) or Automatic Public Key (APK) for encryption keys, and Group Keys for the establishment of User Groups. The Sectéra vIPer Phone provides additional cryptographic capabilities that are discussed in the *Sectéra vIPer Phone Supplement*.

All General Dynamics security products are designed and manufactured to meet General Dynamics' precise specifications and world-class quality standards. During development, our laboratory testing team performed rigorous durability and compliance tests. We are confident that the vIPer Phone meets your own exacting standards.

NOTE: The PSTN Connect accessory provides single line / single appearance capability. The **LINE, HOLD,** *and* **CONF** *keys on your phone are disabled for PSTN operation.*

Thank you for purchasing the vIPer Phone from General Dynamics, a global leader in secure communications technology.

[1] SCIP was previously known as Future Narrow Band Digital Terminal (FNBDT).

Enjoy your new vIPer Phone!

CONSULT WITH YOUR LOCAL SECURITY AUTHORITY FOR SECURITY PROCEDURES APPLICABLE TO THE CONTROL AND USE OF THE vIPer PHONE.

Export of the vIPer Phone is restricted in accordance with the export regulations of the United States.

1.1 Safety Information

Read all of this safety information before using your vIPer Phone.

CAUTION
CONTAINS PARTS AND ASSEMBLIES SUSCEPTIBLE TO DAMAGE BY ELECTROSTATIC DISCHARGE (ESD).

⚠

Only use the vIPer power converter that was provided with the phone. **Do not** use a non-vIPer power converter with the phone. If necessary, contact *Sectéra Product and Sales Information* (page 97) to obtain a replacement vIPer power converter.

⚠

CAUTION - The vIPer Phone contains a lithium battery. While this lithium battery is not intended to be replaced by you, it is important to be aware that the disposal of this lithium battery must be in accordance with local area regulations.

LA PRUDENCE - Le Téléphone de vIPer contient une pile de lithium. Pendant que cette pile de lithium n'est pas projetée être remplacée par vous, c’est important d'être conscient que la disposition de la pile de lithium doit être conformément aux règlements de domaine locaux.

VORSICHT – Das vIPer Telefon hat eine Lithiumbatterie. Es wird nicht beabsichtigt, dass der Anwender die Batterie ersetzt. Es ist allerdings wichtig, dass Sie wissen, dass die Lithiumbatterie nach den lokalen Vorschriften entsorgt werden muss.

WARNING: Lithium batteries contain hazardous and reactive materials. Dispose of in accordance with all proper local, state, and federal regulations. Do not dispose of in uncontrolled trash. Improper handling or high environmental temperature may result in internally generated heat, fire, explosion, or the release of toxic materials and gases.

NOTICE: This equipment meets network protective, operational and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). This is confirmed by marking the equipment with the Industry Canada certification number. This certification does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to their network infrastructure. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions might not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier.

Users should ensure for their own protection that the electrical ground connections of the power utility and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

CAUTION: Users should not attempt to make such connection themselves, but should contact the electric inspection authority, or electrician, as appropriate.

CAUTION: As with any electrical device, be aware that electrical shock may occur if the phone is used near water or during an electrical storm. There is a risk of explosion associated with use of any electrical equipment near explosive gasses.

CAUTION: The vIPer Phone may cease to function during a power outage. You are advised to assess your emergency telecommunication requirements and provide alternate emergency telecommunication equipment if needed.

1.2 Symbols and Fonts Used in this Guide

This guide uses various typefaces and paragraph formats to identify special information of interest to the reader.

Keystrokes that are to be entered on the keypad are shown using the **Keystroke Font**.

Characters that are shown on the display are shown using the **Display Font**.

NOTE: This style is used for notations that are of special interest to the reader.

WARNING: This style is used to call attention to items that may adversely affect the operation of the phone or place the user at risk.

TIP: This style is used to convey information that may save you time and effort.

1.3 Introduction

The vIPer Phone illustrated in *Figure 1.3-1* was designed to be a fully featured phone that provides you with the highest level of security obtainable. The vIPer Phone can operate on the Public Switched Telephone Network (PSTN) when used in conjunction with the PSTN Connect accessory. This section describes those features at a high level. Later sections cover each feature in detail.

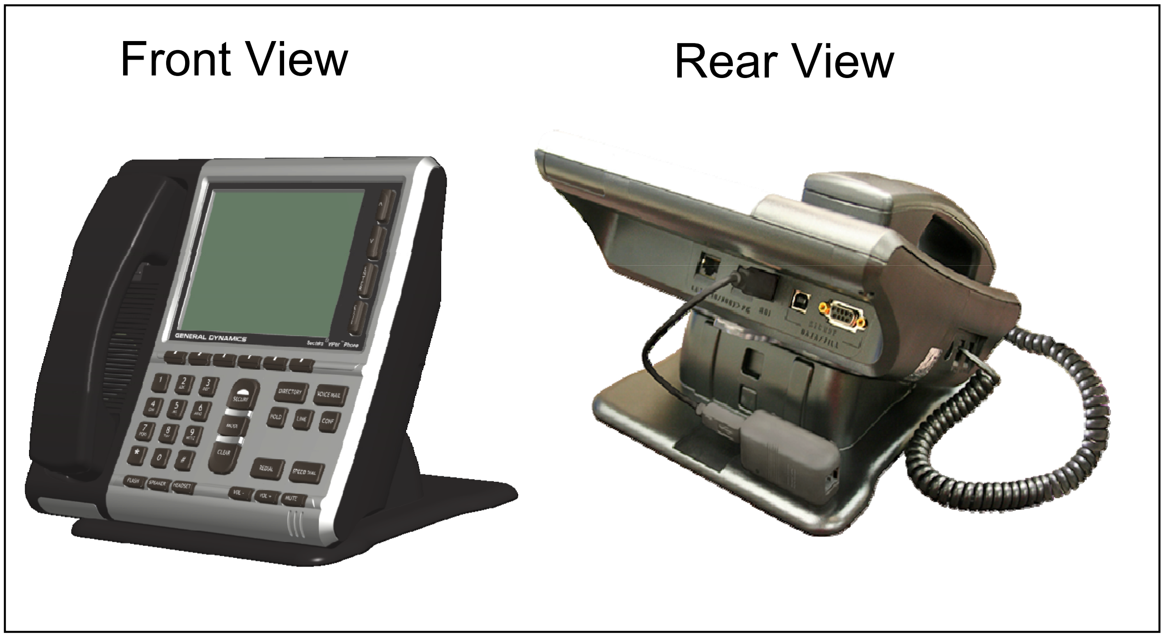


Figure 1.3-1: vIPer Phone

1.3.1 Phone Features

The vIPer Phone is equipped with the following features:

- Clear call capability
- Secure call capability
- High quality speakerphone
- Headset support with optional headset
- Voice Mail support
- Mute
- Flash
- Easy to use menus
- Hearing aid compatibility

The actual features provided by the vIPer Phone may be limited by your network's capabilities. Not all features described in this guide may work at your installation. If you find a feature that does not work as described, the first step is to contact your telecom service provider and determine if the network has that capability.

1.3.2 PSTN Connect -- What You Should Know

The vIPer Phone can operate on analog telephone lines using the PSTN Connect accessory. There are several differences between operating the vIPer Phone in PSTN mode and IP mode. IP telephones locally provide many services such as hold and call transfer. PSTN phones rely on the carrier's switch or local Private Branch eXchange (PBX) to provide these services. Carriers refer to these services as vertical services, and a vertical service is invoked with a vertical service code. Vertical services are standardized in the North American Numbering Plan (NANP), though there is no guarantee that your carrier adheres strictly to the NANP.

Because the vIPer Phone and PSTN Connect are designed for world-wide application and even U.S. carriers do not adhere strictly the NANP standard, there has been no attempt to map vertical services to the special function keys (e.g. **HOLD**, **CONF**, **LINE**). These keys are disabled on the vIPer Phone during PSTN operation.

The vertical services available to you depend entirely on what is enabled on your line by your carrier. You can contact your local carrier to find out what services are available in your area and what are enabled on your line. If you are connected to a PBX (typical of office installations), contact your telephone service department to learn what services are available and how to use them.

1.3.3 Other Documents

The following documents can be found on the CD distributed with your phone.

1.3.3.1 Sectéra vIPer Phone Supplement

If you have a Sectéra vIPer Phone, you should also read the *Sectéra vIPer Phone Supplement* to learn how to use the additional features provided. This supplement is not provided on the distribution CD unless you purchased a Sectéra vIPer Phone.

1.3.3.2 Sectéra and TalkSECURE vIPer Phone Administrator's Manual

The *Sectéra and TalkSECURE vIPer Phone Administrator's Manual* provides information on installing the PSTN Connect network software on your vIPer Phone. The other information in this manual does not apply to PSTN operation.

1.3.3.3 Sectéra and TalkSECURE vIPer Phone Software Update User's Manual

The *Sectéra and TalkSECURE vIPer Phone Software Update User's Manual* provides instructions on updating the cryptographic software of the vIPer Phone. Due to specific security requirements, the process of updating the cryptographic software is different from that used to update the network processor software.

The network software upgrade process is described in detail in the *Sectéra and TalkSECURE vIPer Phone Administrator's Manual*. See *Updating Network Software* (page 83) in this guide for more general information.

1.3.3.4 Group Key Manager Tool User's Manual

The Group Key Manager Tool is a PC-based tool used to generate and distribute Group Key. Group Key, used properly, limits who can talk to whom. More information on Group Key can be found in *Advanced Features* (page 34) and in the *Group Key Manager Tool User's Manual*.

2 Installation

This section discusses how to connect your vIPer Phone to your network.

2.1 Before You Start

Before you connect your vIPer Phone to your network you should contact your carrier or local telephone support department to determine the following things:

1. Is your line a standard analog telephone line that is active? The PSTN Connect will not work on digital or ISDN lines.
2. What is the phone number assigned to this line?
3. What vertical services (e.g. hold, call waiting, call forwarding) are enabled on your line and how do you use them?

Once you have answers to these questions, you are ready to go.

2.2 Packing List

If you ordered a vIPer Phone with PSTN Connect, you should have received the following items:

- vIPer Phone
- Two Ethernet cables
- Power adapter
- AC power cord
- Distribution CD
- Handset
- Coiled handset cord
- Tilt base
- PSTN Connect accessory
- RJ-11 phone cable
- USB cable
- Adhesive pad

If you ordered PSTN Connect separately, you should have received:

- PSTN Connect accessory
- RJ-11 phone cable
- USB cable
- Distribution CD
- Adhesive pad

2.3 Accessories

General Dynamics provides the following accessories that will enhance the usefulness of your vIPer Phone. Contact *Sectéra Product and Sales Information* (page 97) to purchase any of the accessories discussed below.

2.3.1 PSTN Connect

The PSTN Connect allows for operation on a standard analog phone line instead of an IP network. The PSTN Connect accessory includes a USB cable for connection to the Black Digital Interface (BDI) port and a phone cord for connection to an analog phone line jack.

A vIPer Phone in PSTN mode with an attached PSTN Connect accessory has been tested to TSG-5 requirements and is approved for use where on-hook microphonics is a security concern. The PSTN Connect accessory has also been approved for connection to telephone networks in the U.S., Canada, Europe, Australia, and New Zealand.

2.3.2 Push-to-Talk Handset

A push-to-talk (PTT) handset is available for use in high noise environments or for applications with special security requirements. When the PTT switch is released (in its normal position), the audio path from the handset to the phone is disrupted and the vIPer Phone sends audio silence frames over the network. When the PTT switch is depressed, the audio path is completed and normal voice is transmitted over the network. The PTT switch only affects the outbound audio from your phone, and only the audio from the handset. The PTT switch cannot, for example, be used to mute audio from a headset.

The PTT handset is also hearing aid compatible. The handset is shown in *Figure 2.3-1*.

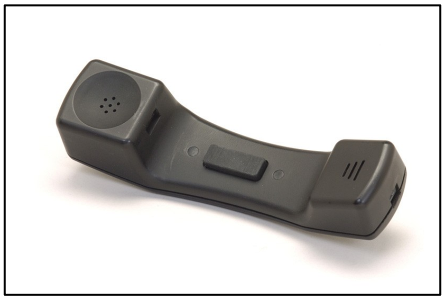


Figure 2.3-1: Push-to-Talk Handset

2.3.3 Headset

A monaural headset with microphone is available (see *Figure 2.3-2*). This headset is designed for use in applications where the background noise is high and is optimized for VoIP applications. The headset comes with a detachable cord that is designed to separate if you should leave your desk without first unplugging from the phone. The headset should be connected to the Headset connector on the left side of the vIPer Phone. When worn, the microphone should be positioned within one-half inch of the wearer's lips for best performance. Placing the microphone below the lips will reduce popping and breath noise when in use.

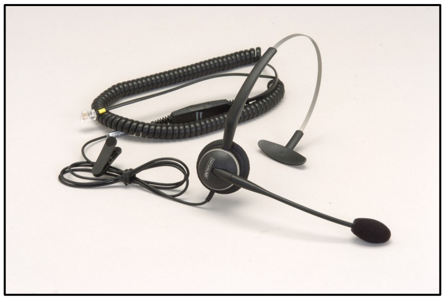


Figure 2.3-2: Headset

When the headset is in use, calls are initiated and answered by pressing the Headset button. Calls are terminated by pressing the Headset button a second time.

Calls can be transferred between the headset, handset, and speakerphone by either pressing a button or lifting/replacing the handset.

2.3.4 Software Update Cable

A software update cable is available if you need to update the security software of your phone. Refer to *Figure 2.3-3.*

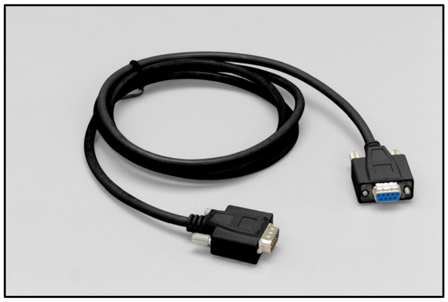


Figure 2.3-3: Software Update Cable

> *NOTE: A standard 9-pin RS-232 serial cable can be used to update your security software. Do not use a null modem cable.*

2.3.5 Additional Items

You may order power supplies, power cords, standard handsets, and Ethernet cables by contacting *Sectéra Product and Sales Information* (page 97).

2.4 Mounting

The vIPer Phone can be placed on a desktop or mounted on a wall.

2.4.1 Desktop

A tilt base is provided for desktop use. The base provides three viewing angles for your convenience. *Figure 2.4-1* illustrates the tilt base assembly.

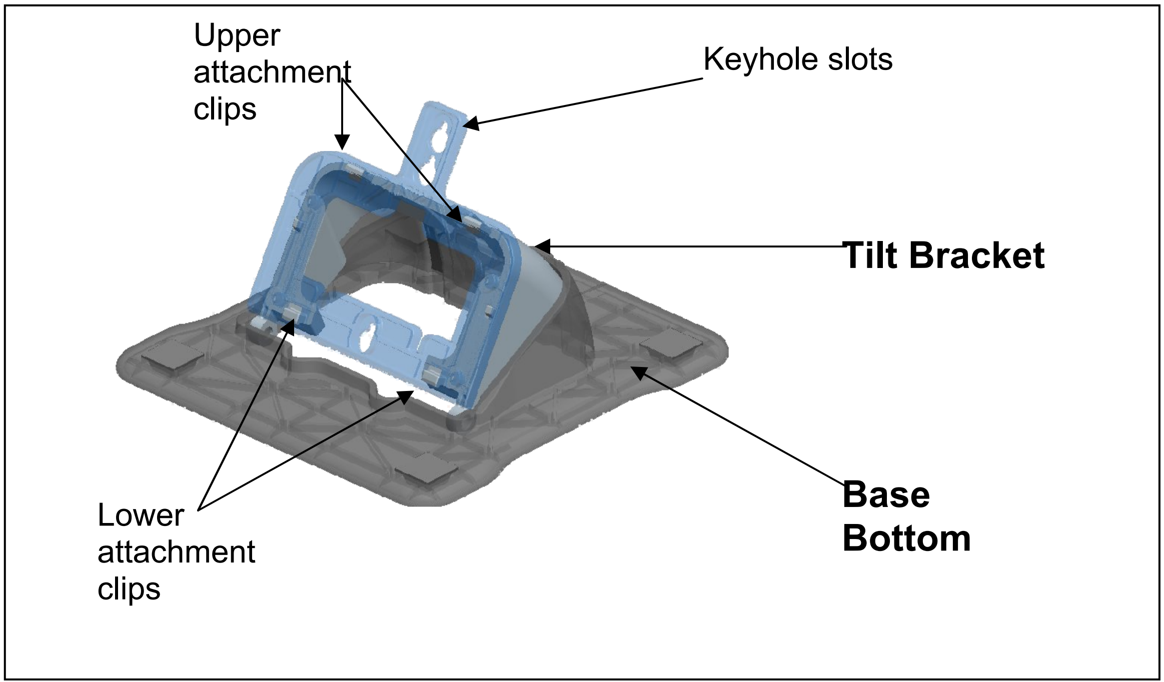


Figure 2.4-1: Tilt Base Assembly

The Mounting Bracket comes attached to the bottom of the vIPer Phone. It may be removed, if needed, but under normal circumstances should remain attached to the phone.

To attach the Tilt Base assembly to the vIPer Phone, slide the assembly onto the back of the phone such that the lower attachment clips engage the slots in the lower portion of the Mounting Bracket. Then press the Tilt Base assembly against the phone so that the upper attachment clips engage the Mounting Bracket.

To remove the Tilt Base assembly, depress the upper attachment clips while pulling the Tilt Base down and away from the phone.

NOTE: The Tilt Bracket may become disengaged from the Base Bottom during shipping. If this should occur, insert the Tilt Bracket into the Base Bottom from below, lightly squeezing the Tilt Bracket so that the holes at the narrow end of the Tilt Bracket can engage the pins on the Base Bottom at the pivot point, and pivot the Tilt Bracket into position so that it is engaged in the Base Bottom.

For desktop use with the PSTN Connect accessory, the PSTN Connect should be attached to the Base Bottom in the left rear corner using the adhesive pad provided as shown in Figure 2.4-2. The phone and module have been TSG-5 tested in this configuration and compliance is assured if the module is mounted as shown.

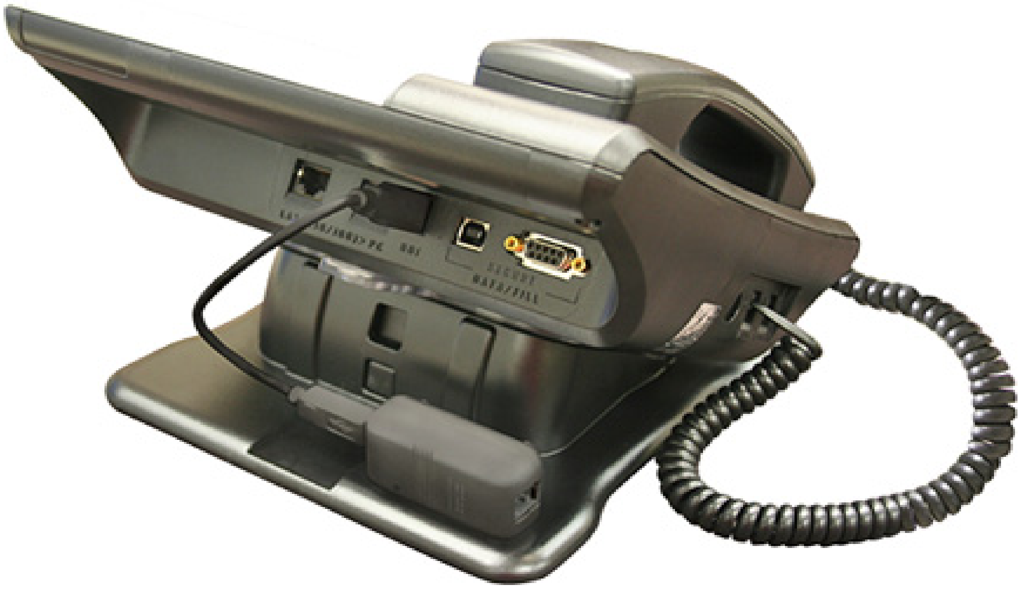


Figure 2.4-2: PSTN Connect Placement

2.4.2 Wall Mounting

The Mounting Bracket comes with three keyhole slots to facilitate wall mounting. The slots are positioned such that they will engage the pins on conventional telephone style wall bracket plates, such as ATBK-VoIP from AllenTel (http://www.allentel.com). Alternately you may screw two number 8 sheet metal screws (not supplied) into the wall to engage the keyhole slots. Only the lower and one of the upper slots need be engaged. Use appropriate wallboard anchors if you are mounting the phone to wallboard.

For wall-mount use with the PSTN connect accessory, the PSTN Connect can be adhered to the wall with the adhesive pad or allowed to dangle. TSG-5 compliance cannot be assured in this configuration however as TSG sensitivity can be affected by mounting location. General Dynamics recommends that the vIPer Phone be desk mounted if PSTN Connect is to be used in a TSG-sensitive environment.

2.5 Electrical Connections

2.5.1 Handset and/or Headset

Connect your handset to the phone using the coiled handset cord provided in your package. Insert one end of the cord into the connector at the base of the handset. Insert the other end of the cord into the connector labeled “HANDSET” on the left side of the phone.

The handset is hearing aid compatible. You may be required to change a setting on your hearing aid to take advantage of this feature.

If you purchased the optional headset you will notice that the headset comes with a separable cord. Connect the separable cord to the headset by mating the flat connector on the cord with the flat connector on the headset. Connect the other end of the cord to the connector labeled "HEADSET" on the left side of the phone. The headset cord is designed to separate should you walk away from the phone while wearing the headset. The cord may have an integral switch with positions numbered 1 through 8. Set the switch to the number 1 position using a straightened paper clip.

2.5.2 Network and Power

The telephone network connection is made using the PSTN Connect accessory. Plug one end of the provided phone cord into the PSTN Connect accessory and the other end into your local analog phone jack. Then plug the PSTN Connect accessory into the phone's BDI connector using the provided USB cable.

The vIPer Phone must still receive power from the Power Adapter. Use one of the provided Ethernet cables to connect the 10/100 LAN port of the phone to the PWR LAN-OUT connecter of the Power Adapter. Connect the AC power cord to the Power Adapter and plug it into a convenient wall outlet. See Figure 2.5-1. DO NOT make any connection to the LAN IN connector of the power converter.

WARNING: The vIPer phone cannot be used simultaneously as an IP phone and a PSTN phone. Only one network (IP or PSTN) should be connected at any time. While no harm will come to the phone if two networks are connected, it is not tested nor certified to be operated in this manner and to do so may risk exposure of sensitive information.

The network supported (IP or PSTN) is determined by the software loaded on the phone. It is possible to switch between networks, but only by obtaining and loading the correct software.

NOTE: The 10/100 PC Port is disabled during PSTN operation.

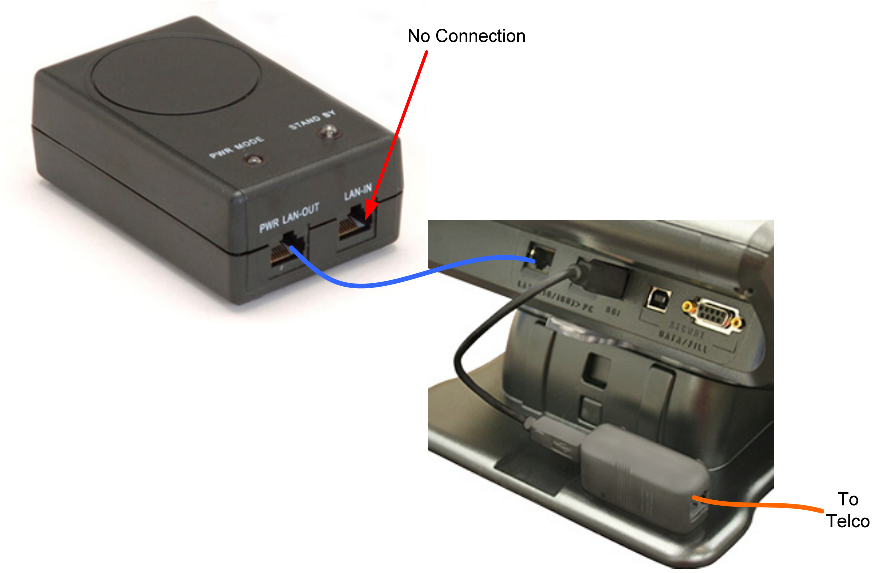
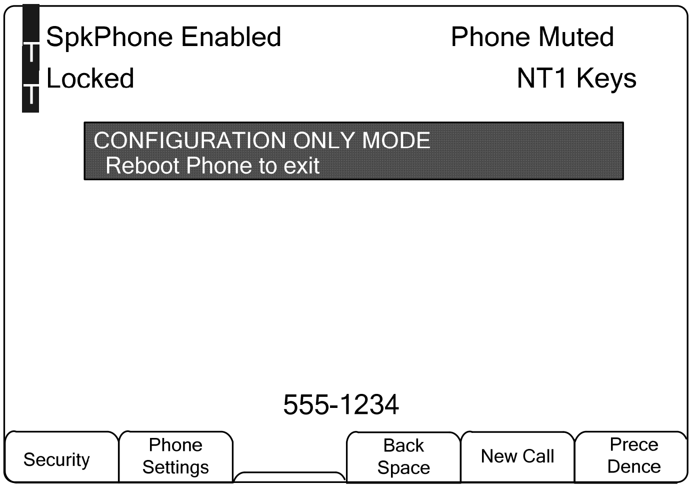


Figure 2.5-1: Phone Connection

2.6 Configuring the Phone

For PSTN operation, you may optionally customize your vIPer Phone's configuration such as your local phone number and number to dial when the **VOICE MAIL** key is pressed. See *Telco Settings* (page 81) for more details.

The vIPer Phone also provides a Configuration Only mode if the PSTN Connect accessory is not present or not properly connected. Select the **Continue** softkey when that error message is displayed to place the phone in Configuration Only mode. In this mode, all of the menus are accessible for phone configuration as shown in Figure 2.6-1, but calls cannot be placed or received.



SpkPhone Enabled Phone Muted
Locked NT1 Keys

CONFIGURATION ONLY MODE
Reboot Phone to exit

555-1234

Figure 2.6-1: Configuration Only Mode

3 Getting Acquainted

3.1 The Keypad

Figure 3.1-1 illustrates the functional key groupings of the vIPer Phone.

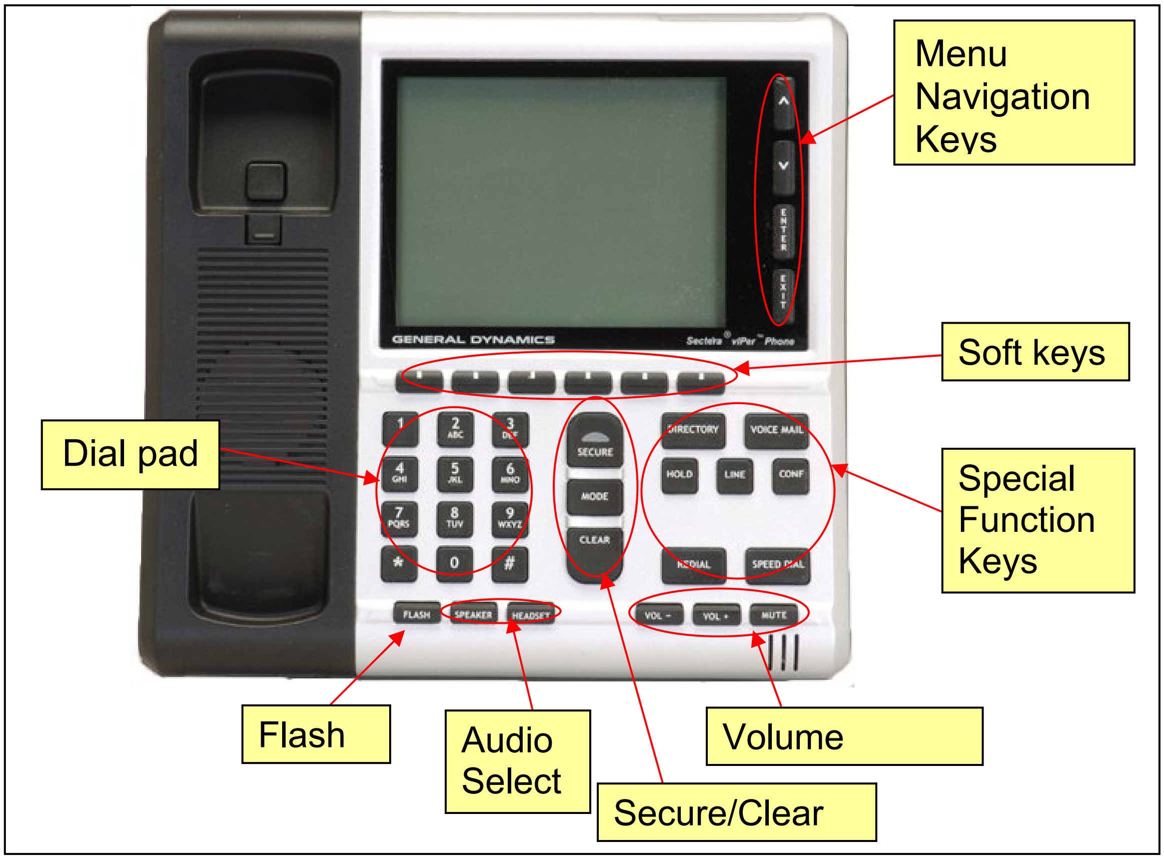


Figure 3.1-1: Functional Key Groupings

The phone keys are organized in functional groupings, as follows:

- The Dial pad is used to dial phone numbers and enter information into the phone. Both on-hook and off-hook dialing are supported.
- The **FLASH** key is used to access additional calls if your network supports this capability. See *Managing Calls* (page 34) for more information.
- The Audio Select keys select either the headset or speakerphone as the active audio device. Lifting the handset off its cradle will disable the speakerphone or headset and route audio to the handset.
- The **SECURE**/**CLEAR** keys are used to transition to and from secure calls. The **MODE** key on the *Talk*SECURE vIPer Phone is reserved for a future application and presently has no function. Users of the Sectéra vIPer Phone should consult the *Sectéra vIPer Phone Supplement* for information on the use of this key.
- The Volume Control keys increase or decrease the volume of the current active audio device. If there is no active call these keys change the ringer volume. The **MUTE** key disables outbound audio, so the party on the other end of the call will

not hear anything from your phone, but you can still hear the other party. You can verify that the line is muted on the call appearance status display (see *Figure 3.2-1*). **MUTE** has no effect on the ringer.

- The Special Function keys activate special features in your vIPer Phone.
  - **DIRECTORY** invokes the directory services menu.
  - **VOICE MAIL** is used to initiate contact with a voice mail server on networks so equipped.
  - **HOLD** is not supported in PSTN mode. Your carrier may provide a hold function that can be invoked with a vertical service code. For more information contact your telecom support personnel or local carrier.
  - **LINE** is not supported in PSTN operation.
  - **CONF** is not supported in PSTN operation.
  - **REDIAL** dials the last dialed number. Note that if you are using Precedence dialing, Redial will use the same priority as when you originally dialed the number. See *Changing the Precedence of Your Call* (page 24).
  - **SPEED DIAL**, followed by a number (0-9) dials one of 10 pre-entered speed dial phone numbers. Pressing **SPEED DIAL** will bring up a list of the currently stored numbers for easy reference, from which you can choose one by entering a digit (0-9), or by using the scroll and enter menu navigation keys.
- Soft Keys. Your phone is equipped with six context-sensitive soft keys. Initially, they are used to invoke different menus provided by the phone. Their function changes as you navigate the phone's menu structures. The display is not touch sensitive. To activate these soft key, you must select the keys located below the display. See *Figure 3.1-1.*
- Menu Navigation Keys are used to navigate the menus and accept or reject actions.

TIP: Occasional menus will provide Yes/No or True/False soft keys. You may use the **ENTER** navigation key interchangeably as **Yes** or **True** and the **EXIT** navigation key as **No** or **False**.

TIP: You may rapidly page through long lists of data by holding down the up or down navigation keys. You may also scroll to a specific entry by entering the number associated with that entry (e.g., in a 200 item list, entering "5" "0" will scroll to entry number 50).

3.2 The Display

Initially, your phone will be at the Top Level On-Hook Display, which is illustrated in *Figure 3.2-1*.

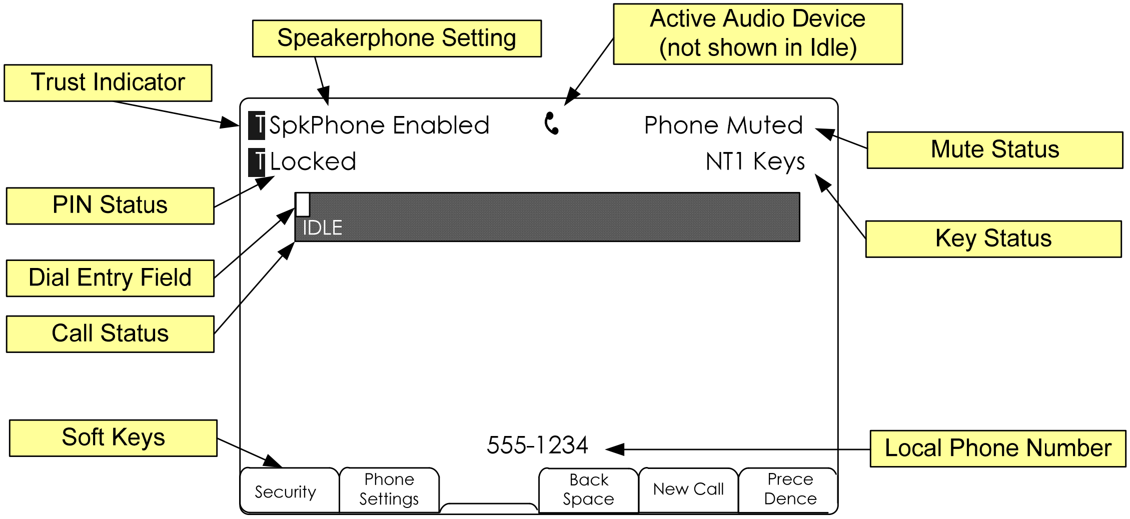


Figure 3.2-1: Top level On-Hook Display

The first two lines are used by the Secure Call Processor to display status information. They provide important information on the security status of the phone.

- Speakerphone status indicates whether use of the speakerphone is allowed or not (not whether the speakerphone is active at the moment). If showing **SpkPhone Enabled**, the speakerphone may be used in an active call. If showing **SpkPhone Disabled**, the speakerphone may not be used.
- The Phone Mute State, when showing **Phone Muted**, indicates that all microphones (handset, headset, and speakerphone) are disabled. This is normal when the phone is on-hook, and will change to **Phone Unmuted** as soon as the phone is taken off-hook.
- The PIN Status indicates whether a valid User ID and PIN has been entered and is active. When showing **Locked**, the phone cannot be used to make secure calls. Unlock the phone by entering a valid User ID and PIN.
- The Key Status indicates whether keys are loaded. Initially, this area will be blank. Once you have loaded or generated key, it will resemble Figure 3.2-1.

> WARNING: The inverse video T on the first and second line of your display should always be present if the phone is in operational mode and is functioning properly. If you should notice that the T is missing, something may be wrong with your phone and it should not be used for secure calls until you understand why the T is not present.

The inverse video T, hereafter referred to as the Trust Indicator, will appear on other lines from time to time. This behavior is normal and simply indicates that the Secure Call Processor has taken over those lines to display additional information.

NOTE: The Trust Indicator identifies the source of the data on your phone's display. When the inverse video "T" appears in the first column, the Secure Call Processor (SCP) is providing the data; otherwise the data is coming from some other source. Information from the SCP can always be trusted, while information from the network processor may not always be trustworthy. While it should not be possible to hack into the vIPer Phone, understanding how the Trust Indicator works adds another layer of protection. For example, if you should see an indication on the display that your call is secure, but if there is no T in the first column of the line showing that message, then your phone may have been compromised. Please report this to your COMSEC Custodian or Security Administrator, as well as to Customer Support (page 95).

The remaining lines on the display are shared between the menu system and the call appearance status indicators. The PSTN Connect software only supports a single call appearance.

The local phone number may be displayed just above the soft key labels. To learn how to configure this number, see *Local Phone Number* (page 82).

NOTE: If a fault occurs in non-trusted subsystems (e.g., "Error <8 digit alphanumeric code> Reboot Phone"), it will be shown on the same line as the local phone number. Record the number, cycle power on the phone (unplug and reconnect the Power Adapter), and if the problem persists call Customer Support.

The tabs below the phone number are context-sensitive soft key labels. Soft keys can be used to invoke menus, for editor functions, and for confirmations (yes/no) depending on where you happen to be in the menu. The soft keys can also be used to start, answer, and end calls depending on the state of the current call.

3.3 Text Entry

The dialpad is used to enter text, such as when entering a name while creating a new Personal Contacts entry.

Table 3.3-1 identifies the special characters that are mapped to the numeric dialpad when you enter text. Letters are mapped to the numbers 2 through 9 just like on a regular telephone. Punctuation characters are mapped to **1**, *, **0**, and **#**, but these mappings are not printed on the keycaps[2].

Table 3.3-1: Key Character Map

Key	Character Map
1	1 : ; (one, colon, semicolon)
2	2 A B C a b c
3	3 D E F d e f
4	4 G H I g h i
5	5 J K L j k l
6	6 M N O m n o
7	7 P Q R S p q r s
8	8 T U V t u v
9	9 W X Y Z w x y z
*	* . @ (asterisk, period, 'at' symbol)
0	0 - <space> _ , (zero, hyphen, space, underscore, comma)
#	#

3.4 Menu Navigation

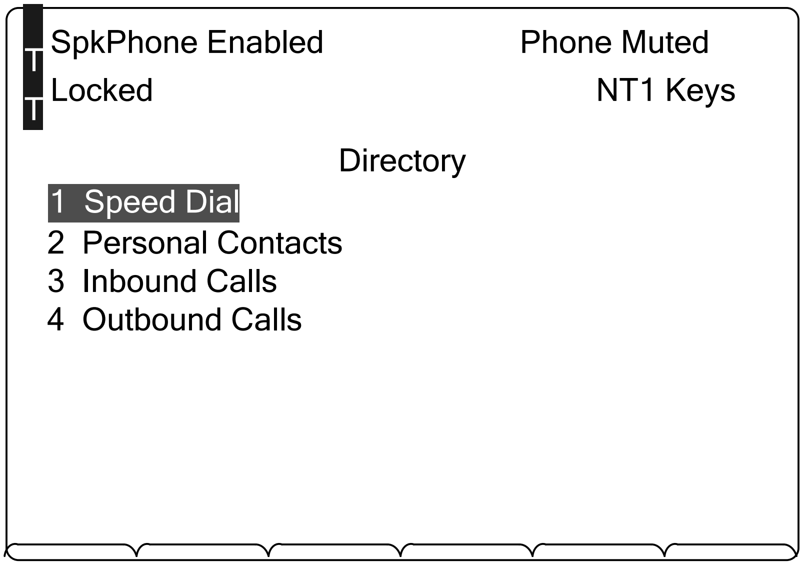
Menus are navigated using the navigation keys (scroll up, scroll down, **ENTER**, and **EXIT**), the soft keys, and the special function keys.

From the Top Level On-Hook Display, you can invoke the following menus:

- The Security Menu via the **Security** soft key
- The Phone Settings Menu via the **Phone Settings** soft key
- The Directory Menu via the **DIRECTORY** key
- The Speed Dial Menu via the **SPEED DIAL** key

For example, if you press the **DIRECTORY** key, you will see the Directory Menu, shown in *Figure 3.4-1*.

[2] There is some logic to the punctuation key assignments. Here is a suggestion that may help you remember: The 1 key special characters are skinny and vertical (: and ;). The * key special characters are round (. and @). The 0 key special characters fill space, but don't do anything (- space _ ,).



SpkPhone Enabled Phone Muted
Locked NT1 Keys

Directory

1 Speed Dial
2 Personal Contacts
3 Inbound Calls
4 Outbound Calls

Figure 3.4-1: Directory Menu

Menus are implemented as numbered lists. The first item in the list is highlighted with inverse video, and it can be selected by pressing **ENTER**. You can scroll up or down using the scroll arrows to select a wanted menu item, or alternately you can just press the number associated with the menu item. For example, if you wanted to access the Outbound Call history, you could either:

- Press **<scroll down>**, **<scroll down>**, **<scroll down>**, **ENTER**; or
- Press **4**

TIP: Learn to use the number shortcut keys; they will save you time.

Use the **EXIT** key to back out of a menu.

NOTE: After a period of inactivity in a menu the vIPer Phone will revert to the next higher menu. After a similar, second period of inactivity, the vIPer Phone will exit the menu system and show the Top Level On-Hook display. This behavior is normal.

The vertical scroll keys are also used to navigate long lists. Depressing a scroll key momentarily moves the cursor up or down one line. Holding down a scroll key causes the display to scroll one page at a time (approximately 10 lines per page).

3.5 Menu Summary

The menu structure of the vIPer Phone is shown in *Figure 3.5-1*. The Sectéra vIPer Phone supports additional security menus. Users of the Sectéra Phone should consult the *Sectéra vIPer Phone Supplement* for additional menu details. Each menu function is discussed in detail in *Menus* (page 44).

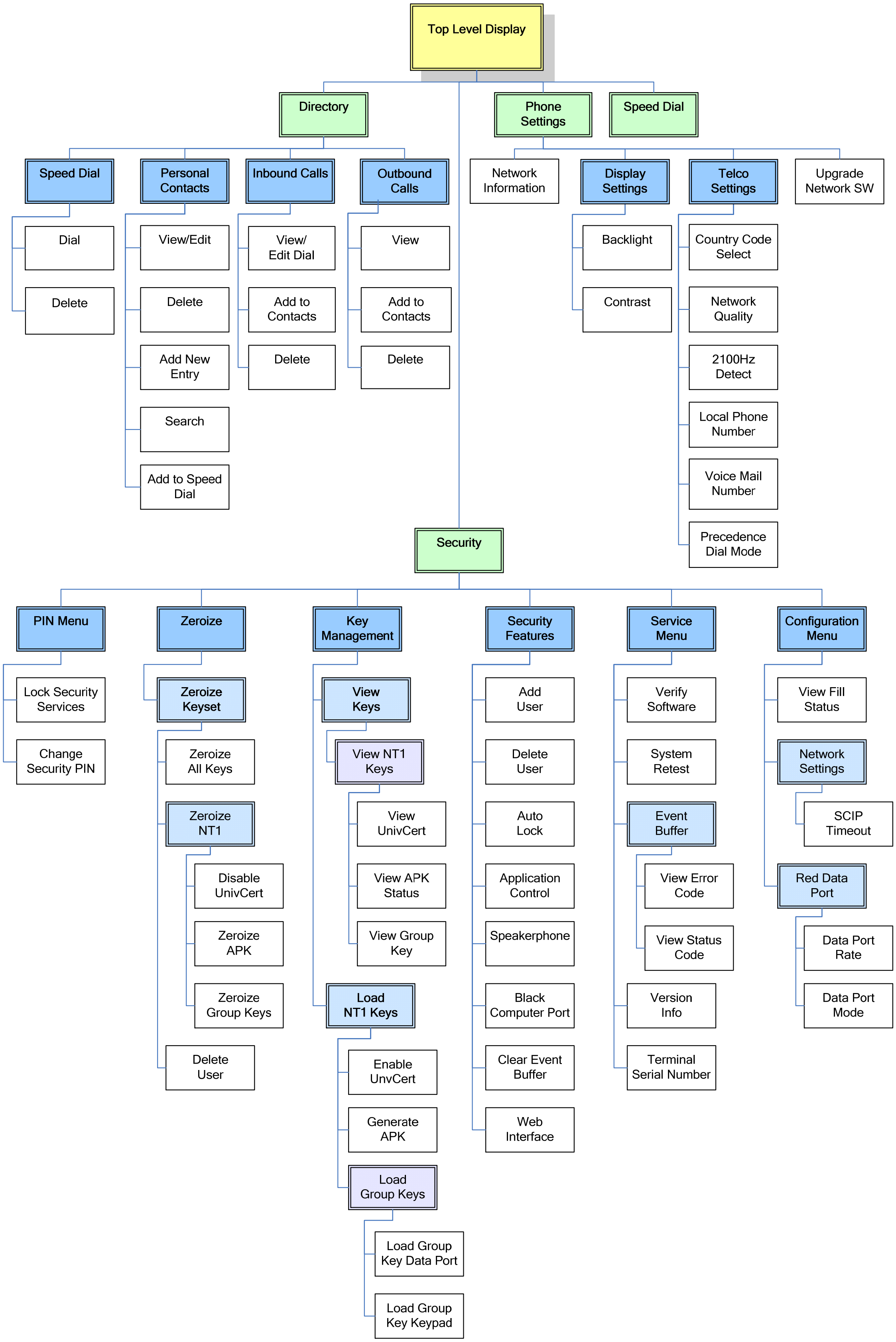


Figure 3.5-1: Menu Structure

3.6 Make a Clear Call

There are many ways to initiate a call, but they are all variations on two themes: off-hook dialing and on-hook dialing.

Off-hook dialing is what you do with an ordinary phone. While off-hook dialing is easy and what we are all used to, there are some good reasons to start using on-hook dialing.

The difference between on-hook and off-hook dialing is in the details. The main difference you will see is that you can edit the dial string when you dial on-hook, but you cannot when you dial off-hook. If you enter a wrong digit on-hook you can correct the error without having to hang up.

NOTE: The speakerphone capability of your vIPer Phone may be disabled for security reasons.

3.6.1 Dialing a Call

Clear calls may be dialed either off-hook (like a conventional phone) or on-hook (like a cell phone).

3.6.1.1 Off-Hook Dialing

The steps for off-hook dialing are:

1. Take the phone off-hook by lifting up the handset or momentarily depressing the **HEADSET** or **New Call** softkey or **SPEAKER** key if speakerphone is enabled.
2. Wait for dial tone, then dial the number.
3. Do one of the following to end the call:
    a. Place the handset back on its cradle if you are using the handset.
    b. Momentarily depress the **HEADSET** key if you are using the headset.
    c. Momentarily depress the **SPEAKER** key if you are using the speakerphone.
    d. Press the **End Call** softkey.

3.6.1.2 On-Hook Dialing

The steps for on-hook dialing are:

1. Enter the dial string. When you enter the first digit the top level display changes as shown in *Figure 3.6-1*. The << and >> scroll arrows, combined with **Backspace**, permit editing of the dial string
2. Do one of the following to initiate the call:
    a. Lift the handset for a normal phone conversation.
    b. Press **SPEAKER** to use the speakerphone capability if speakerphone is enabled.
    c. Press **HEADSET** to use your headset.

d. Press the **New Call** softkey or **ENTER**. This feature will only work if the speakerphone is enabled for use.

3. Do one of the following to end the call:
   a. Place the handset back on its cradle if you are using the handset.
   b. Momentarily depress the **HEADSET** key if you are using the headset.
   c. Momentarily depress the **SPEAKER** key if you are using the speakerphone.
   d. Press the **End Call** softkey.

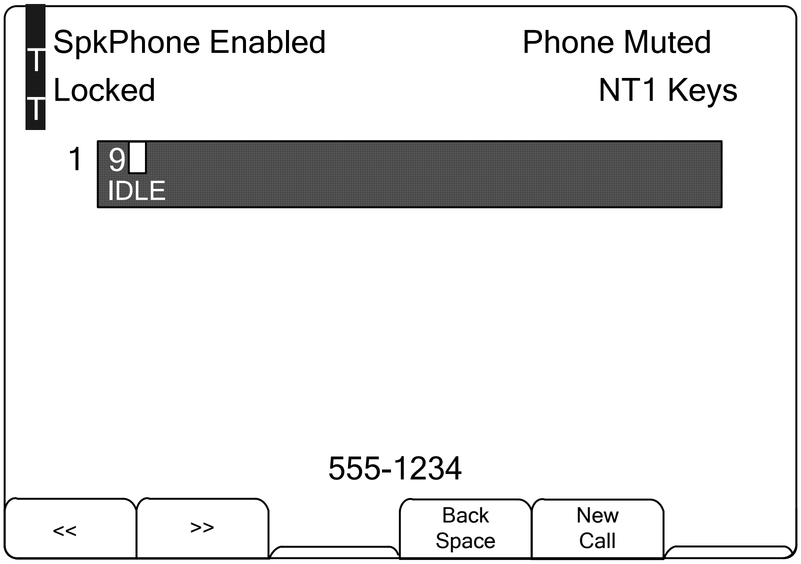


Figure 3.6-1: On-Hook Dial Display

3.6.1.3 Changing the Precedence of Your Call

Some networks support precedence dialing. This feature goes under various names, such as MLPP (Multi-Level Precedence and Preemption) and FoFIP. Precedence is the priority associated with a call (e.g. Flash Override, Flash, Immediate, or Priority). Preemption is the process of ending an existing, lower priority call to allow a higher priority call to be accepted.

If your network supports precedence dialing and you are allowed that capability, you can prioritize your call. The vIPer Phone supports two methods of precedence dialing, configurable using the Telco Settings menu, both of which require that you select the precedence level of the call before dialing the number of the person you are calling. For more information on configuring the precedence dialing method, refer to *Precedence Dial Mode* (page 82).

If your phone is configured for prefix dialing, simply dial the precedence digit(s) specified by your network provider. If your phone is configured for menu precedence dialing, the precedence soft keys will appear. To make a priority call using softkeys, press the Precedence soft key (see *Figure 3.6-1*). The priorities are:

A sends a **Flash Override** signal (highest priority).

B sends a **Flash** signal (second highest priority).

C sends an **Immediate** signal (third highest priority).
D sends a **Priority** signal (fourth highest priority).

Select one of the precedence keys and then dial the phone number. Calls made without any priority are given the lowest priority for a phone line.

If a priority call cannot be connected between parties, you might hear one of the following messages:

- An invalid priority level was requested.
- The priority of the call could not be completed because of multiple priority calls of equal or higher value or unavailability of network resources to connect the call.
- The called party's phone is busy and does not support MLPP.

Precedence dialing should be used with caution because it has the potential to deny other legitimate users the ability to make calls.

3.6.2 Answering a Call

When your phone rings, you may answer the incoming call in several ways:

- By lifting the phone's handset,
- By depressing the **HEADSET** key to use a headset,
- By depressing the **SPEAKER** key to use the phone's speakerphone, or
- By pressing the Answer softkey. This feature will only work if speakerphone is enabled for use.

If you are not present when the phone rings, the call will be marked with an asterisk in the Inbound Call list.

If you are on the phone when a call comes in and your telecom service provider has set up Voicemail, the call will go to Voicemail.

If you are on the phone when a precedence call comes in, see *Preemption of an Existing Call* (page 34).

3.7 Security Features

This section discusses features common to the Sectéra and *Talk*SECURE vIPer Phones. Users of the Sectéra vIPer Phone should consult the *Sectéra vIPer Phone Supplement* for a more detailed explanation of the capabilities of their phone.

Your vIPer Phone adheres to the Secure Communications Interoperability Protocol (SCIP) standard. SCIP is a cryptographic, key agreement, and communication protocol developed by the United States and other governments to provide interoperable secure communications.

3.7.1 Access Control Models

The vIPer Phone contains access control features that restrict operation of the phone's security features to authorized users only.

The Security Administrator is responsible for selecting one of the three local user access control models supported by the vIPer Phone. The three access control models are:

1. Uncontrolled requires no User ID or PIN to access security features.
2. Controlled permits a maximum of three User IDs with PINs, each user having the same privileges and access to security features.
3. Restricted permits a maximum of one Master User ID and PIN and two User IDs with PINs. The Master User has access to some security features that are blocked from the regular users.

> *NOTE: A PIN is a Personal Identification Number, and works like a password on a computer. You should not give your PIN to other people unless authorized by your Security Administrator.*

Table 3.7-1 on page 28 shows access privileges associated with each access control model.

If you invoke the Controlled or Restricted access control models, when you access a feature that requires PIN access you will be prompted to supply your one digit UserID and six digit PIN. You have four opportunities to enter your UserID and PIN correctly. On the fourth consecutive failed attempt your UserID and PIN are deleted. If this is the last UserID, all keys will also be deleted.

> *NOTE: The number of attempts to enter a PIN is limited to prevent PIN-guessing attacks on the phone.*

The different access control models address different needs.

- If you want anyone to be able to use the phone to place secure calls, you should choose the Uncontrolled model by electing not to create User IDs and PINs.
- If you want only specific people to be able to make secure calls and alter the security settings of the phone, choose the Controlled model by creating User IDs and PINs, but not creating a Master User.
- If you want only one person to be able to modify the security settings of the phone, create a Master User.

> *NOTE: Select a PIN that is easy for you to remember. The vIPer Phone will let you enter any sequence of digits you want for a PIN – the only requirement is that it be six digits long. However, certain PINs are not particularly good if you want to prevent unauthorized people from using your phone. For example:*
> *-- Avoid repeating digits or sequential digits.*

-- Do not use part of your phone number, driver's license number, or other commonly known number.
-- Do not use recognizable patterns, such as 121212.
Check with your Security Administrator for further guidance on PIN selection.

3.7.1.1.1 Uncontrolled Access Control Model

The vIPer Phone's factory default is the Uncontrolled Access Control Model. The Uncontrolled Access Control Model requires no users to be defined and allows anyone to use and change the general security capability of the phone. The phone's Locking and Unlocking capability is not active.

3.7.1.1.2 Controlled Access Control Model

The Controlled Access Control Model is established when the first User ID and PIN is created during *Generate APK* or *Add User* processing and is not made a Master User. Any subsequent user IDs created will have the same access privileges as the first user.

In the Controlled Access Control Model, you are required to enter your User ID and PIN to unlock the phone to access the security functions: PIN Menu, Key Mgmt Menu, Security Menu, Software Update and secure communication. All users that have a User ID and PIN have the same capabilities relative to the security functionality of the phone. Users that do not have a User ID and PIN have limited access to the phone and limited capabilities (e.g., they will not be able to access the Key Management or Security Features menus, perform a Software Update, or make a secure call).

To create users and associated User IDs and PINs, perform the Add User steps in one of the following sections:

- *Add User* (page 59)
- *Generate APK* (page 56)

Following the creation of the first user, the phone is now using the Controlled Access Control Model.

Anyone has access to non-security functionality; see *Table 3.7-1* on page 28 for more information.

3.7.1.1.3 Restricted Access Control Model

For the Restricted Access Control Model, the first User ID and PIN that is created is made a Master User. Only the Master User can access and/or change the security capability under the Security Menu and perform Software Updates. The Master User always has a User ID of 1. Users that do not have a Master or User ID and PIN have limited access to the phone and limited capabilities (e.g., they will not be able to access the Key Management or Security Features menus, perform a Software Update, or make a secure call). Any users created after the Master User will be created as User IDs with PINs.

NOTE: The Master User must be the first user created. If a User ID with PIN has already been created, and he has not been designated a Master User, you cannot create a Master User without first deleting all existing Users and key material.

3.7.1.1.4 Capabilities of each Access Control Model

Capabilities attendant with each access control model are identified in *Table 3.7-1*. The annotations in the table convey the following meaning:

- No PIN – No User ID or PIN is required to access this feature for this access control model. For example, anyone can access clear voice with any access control model.
- User PIN – A User ID and PIN (inclusive of Master User) is required to access this feature for this access control model. For example, any person with a User ID and PIN (inclusive of Master) can access secure voice when using either the Controlled or Restricted access control model.
- Master PIN – Only the Master's User ID and PIN can be used to access this feature for this access control model. For example, only the Master User can access software update when using the Restricted access control model.
- N/A – This feature does not appear with this access control model. For example, the PIN Menu does not appear when using the Uncontrolled access control model.

Table 3.7-1: Access Control Restrictions for Various Models

Model **Feature**		**Uncontrolled (No PIN)**	**Controlled (PINs defined)**	**Restricted (PINs defined w/Master)**
Clear Voice		No PIN	No PIN	No PIN
Secure Voice		No PIN	User PIN	User or Master PIN
Software Update		No PIN	User PIN	Master PIN
Menu Access	**PIN Menu**	N/A	User PIN	User or Master PIN
	Zeroize Menu	No PIN	No PIN	No PIN
	Key Management Menu	No PIN	User PIN	User or Master PIN
	Security Features Menu	No PIN	User PIN	Master PIN
	Configuration Menu	No PIN	No PIN	No PIN
	Service Menu	No PIN	No PIN	No PIN
	Phone Settings Menu	No PIN	No PIN	No PIN
	Directory Menu	No PIN	No PIN	No PIN
	Speed Dial Menu	No PIN	No PIN	No PIN

Sometimes a PIN is required to access certain menus, depending on your access control model. If a PIN has already been entered, it will not be asked for again until the Auto

Lock timeout expires. The Auto Lock timeout will expire after a period of inactivity. Once it expires, the cryptographic capabilities of the phone are inaccessible until a PIN is entered again. For more information on the Auto Lock timeout, refer to *Auto Lock* (page 61).

3.7.2 User Management

In any but the Uncontrolled Access Control Model, users may be added or deleted as needed to restrict use of the vIPer Phone's security features.

3.7.2.1 Add Users

Users may be added up to the limit supported by the phone (currently 3, including the Master User). Once User IDs and PINs have been created they should be issued to the responsible persons. See *Add User* (page 59) to learn how to add users.

3.7.2.2 Delete Users

When a user no longer requires access to the phone his User ID and PIN should be deleted. See *Delete User* (page 60) to learn how to delete users.

3.7.2.3 Consequences of Deleting the Master User

It is possible, and desirable under some circumstances, to delete the Master User after creating additional User IDs and PINs. By deleting the Master User, the ability to access security critical functions is removed. This can be a means of preventing unauthorized access to these features when the unit is placed in an environment where compromise is likely and the probability is high that the phone may not be recovered.

3.7.3 Key Management

When the vIPer Phone ships from the factory, it does not contain any encryption key material. An encryption key is required for making secure calls. This section describes the types of keys used by the *Talk*SECURE vIPer. Users of the Sectéra vIPer should refer to the *Sectéra vIPer Phone Supplement* for additional keys used.

The *Talk*SECURE vIPer Phone uses two types of keys with two distinct purposes:

- Encryption key (required) – used to encrypt the phone conversation
- Group key (optional) - used to define User Groups or Communities of Interest among users who share a common encryption key

3.7.3.1 Encryption Key

The vIPer Phone will need to have an encryption key enabled or generated before a secure call can be established.

Two types of encryption key are supported for encrypting phone conversations:

- Universal Certificate (UnivCert) encryption key: Government-defined key used to go secure with General Dynamics and non-General Dynamics terminals. For instructions on enabling the UnivCert encryption key, see *Enable UnivCert* on page 56.

- Automatic Public Key (APK) encryption key: A General Dynamics proprietary key used to go secure with General Dynamics terminals. For instructions on generating the APK key, refer to *Generate APK* on page 56. APK is generated by the phone and does not expire. It may be regenerated at any time. Refer to Section 5.2.3.2.2, *Generate APK*, on page 56 for more information.

At the beginning of each secure call, a Traffic Encryption Key (TEK) is generated by your phone in cooperation with the phone you are calling. The TEK is only used once for each call - then it is discarded. Information from your UnivCert or APK encryption key, the corresponding encryption key of the phone you are calling, and random data are used to form the TEK, so it is different for every call.

On a phone with both a generated APK and an enabled UnivCert encryption key, the phone gives priority to the UnivCert encryption key when establishing a secure call. Such a phone will only fall back to the APK encryption key if the remote terminal as a generated APK encryption key and does not have an enabled UnivCert encryption key.

NOTE: General Dynamics recommends that the APK encryption key be regenerated periodically based on your security policy.

3.7.3.2 Group Key

The Group Key is used in conjunction with the encryption key and allows you to securely communicate with a controlled group of users. Group Key encrypts only call setup information. The vIPer Phone uses a one-time TEK generated during call setup to encrypt the phone conversation.

There are two types of Group Key:

- UnivCert Group Key – Government defined Group Key associated with the UnivCert encryption key
- APK Group Key – General Dynamics defined Group Key associated with the APK encryption key

A central administrator (usually your Security Administrator) defines who belongs to a group and assigns a Group Key to that group. He loads the Group Key into each phone belonging to a group member. The vIPer Phone can hold any combination of up to ten UnivCert or APK Group Keys to allow participation in multiple groups.

Suppose you have three groups called Management, Sales, and Engineering shown in Figure 3.7-1. Everyone in each group needs to be able to talk to members of his own group. In addition, you want Management to be able to talk to Engineering and Sales, but you do not want Engineering and Sales talking to each other. Each group gets their own Group Key; there is a Sales Key, a Management Key, and an Engineering Key. In addition, Management gets the Sales Key and the Engineering Key.

Because Management also has the Sales and Engineering Group Keys, Management can talk securely with those departments. But since Sales and Engineering do not share a Group Key, they cannot talk securely with each other.

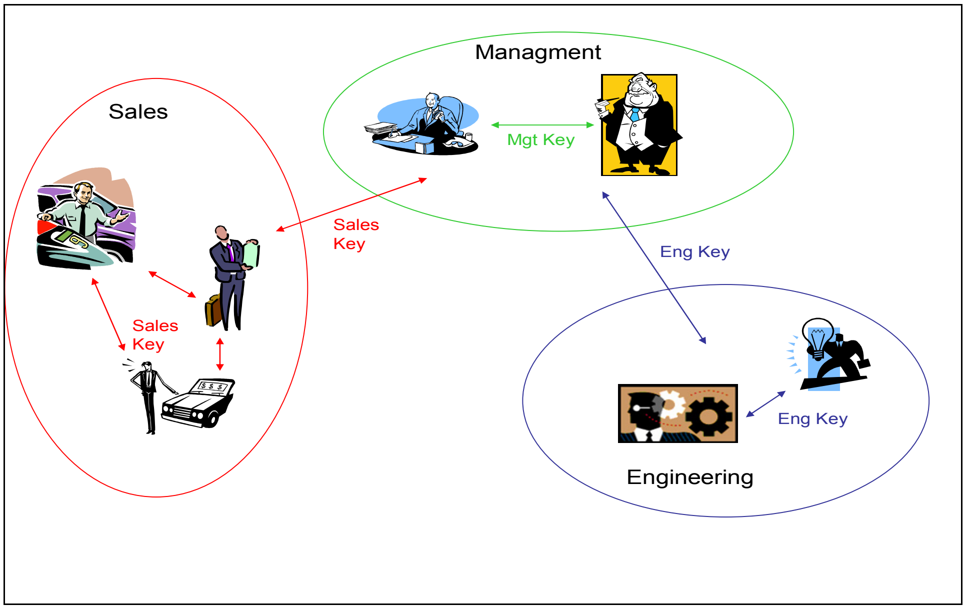


Figure 3.7-1: Group Key Management

When you place a secure call the phone will automatically select a compatible Group Key to speak with the other party; you do not have to select a key. If you do not have a matching key, and all of the Mandatory Exclusion Flags for your keys are set True to deny traffic, you will not be able to speak with the other party. However, if your phone has one of its Group Key Mandatory Exclusion Flags set to False, you will be able to talk securely to a party outside the group by performing a Secure Downgrade to APK.

Group Key is generated and loaded into the phone either by using the Group Key Manager Tool or by manually entering it via the dialpad. The Group Key Manager Tool is a PC based application that is provided on your distribution CD and can also be obtained by contacting *Customer Support* (page 95).

General Dynamics recommends using the Group Key Manager Tool to generate and load Group Key into your phone. The Group Key Manager Tool generates the Group Key and makes it easy to load the same Group Key into several phones.

For more information on developing and loading Group Key, refer to the *Group Key Manager Tool User's Manual*, included on your distribution CD.

For information on loading Group Key, see *Load Group Key* (page 57).

NOTE: General Dynamics recommends that once the vIPer Phone has a Group Key loaded, the user should create User PINs to control access to the vIPer Phone. Without a User PIN, anyone can access and use your vIPer Phone and Group Key. Refer to User Management (page 29) and Access Control (page26).

3.7.3.3 Zeroize

The Zeroize function removes key material from your vIPer Phone. Zeroize is used primarily if you want to load a new key into the phone, if you fear your APK key or Group Keys have been compromised, or if you fear your phone is about to be compromised (e.g. stolen or tampered with).

TIP: It is good security practice to zeroize and regenerate your APK key occasionally. If you are using Group Key, it is also a good idea to generate and distribute new Group Keys periodically. Your Security Administrator can tell you what your organization's policy is regarding key regeneration and distribution.

3.7.4 24 Hour Retest

Your vIPer Phone includes the capability to test its cryptographic components periodically.

The 24 hour retest feature works as follows:

1. Approximately 24 hours after the last power up or retest, the phone checks if there is an on-going call. If there is no call, the phone resets itself, which causes it to go through its built-in tests.
2. If there is an on-going call, the phone waits for the call to end.
3. After the call ends, the phone waits an additional ten seconds. If no call is initiated in that time, the phone resets.
4. If a new call is initiated before ten seconds expires, the phone repeats this process from step 2.

Each time the phone resets it goes through a full suite of security self-tests. To reduce the operational impact of System Retest, cycle power on the phone during off hours so that System Retest also occurs during off hours.

If any subsystem reports a failure, the phone will reset again and attempt to clear the error. If the error cannot be cleared after four attempts, the phone reports the error on the display and waits for a user response. General Dynamics recommends that you note the error code and contact your COMSEC Custodian or Security Administrator if you should ever see an error display.

3.7.5 Mode Change

Users of the Sectéra vIPer Phone should refer to the *Sectéra vIPer Phone Supplement* for additional information on Mode Change (e.g. security level change).

The **MODE** key on the *Talk*SECURE vIPer Phone is provided for future capabilities planned for a later software release.

3.7.6 Depot Return Switch

The Depot Return switch clears all key material from the phone and renders the phone incapable of cryptographic processing when depressed and held for two seconds. It is labeled “DEPOT RTN” and located under the base of the phone. The Depot Return switch operates whether the phone is powered or not and is intended to be used when preparing the phone for return to General Dynamics C4 Systems for repair. The phone must be returned to restore cryptographic capability once the switch is depressed.

The Depot Return switch may be used as a zeroize switch in emergency situations as long as the user is aware that the phone is no longer capable of secure calls until serviced by General Dynamics C4 Systems.

Refer to Section 9.3, *Returns,* on page 95 for more information.

4 Advanced Features

This section describes features provided by your phone and/or network infrastructure. It should be noted that some features, such as voice mail, depend on network support and will not function if your network does not provide these capabilities.

4.1 Managing Calls

This section provides information on what can be done while in a call.

NOTE: In addition to the features described here, three-way conferencing and call transfer are planned for a future release. The **CONF** *button is reserved for future use and has no affect on your phone.*

4.1.1 Preemption of an Existing Call

Your network may support call preemption. If so, and your call is being preempted, you will hear a preemption tone and your current call's channel will be torn down immediately (you will have no voice). You must place the phone on-hook at which time, if you are the person who is being called, your phone will ring and you may answer. See *Changing the Precedence of Your Call* (page 24) for information on how to make a precedence call.

4.1.2 Audio Device Selection

Your vIPer Phone is equipped with three audio devices, or ports – a handset, a headset (optional), and a speakerphone. As you have already seen, you can use any of them to initiate a call. You can also switch between them during a call. The switching works as follows:

- If you are using the handset and press **SPEAKER** or **HEADSET**, the speakerphone or headset will become active. You can then place the handset on the cradle.
- If you are using the speakerphone or headset and lift the handset off the cradle, the handset becomes active immediately.
- If you are using the speakerphone and press **HEADSET**, the headset becomes active.
- If you are using the headset and press **SPEAKER**, the speakerphone becomes active.

The Master User of your phone may elect to disable speakerphone capability if your phone is used in certain environments. If so, the **SPEAKER** key has no effect.

The top line on the display shows an icon indicating which audio device is active. No icon is displayed if all audio devices are inactive.

For more information on speakerphone, see *Speakerphone* (page 42). For more information on the Master User capabilities, see *Security Features* (page 25).

4.1.3 Hold (Clear Calls Only)

The **HOLD** key is disabled during PSTN operation.

4.1.4 Mute

Press **MUTE** to mute outbound audio for the currently active call appearance. Press **MUTE** again to restore outbound audio. When the phone is muted it doesn't send out any audio, but it still receives audio from the other phone. The caller at the far end will hear nothing, but you will still be able to hear him. Mute works during both clear and secure calls. This is important to remember since the transition between clear and secure calls will maintain the current mute state of the phone. Mute always consumes bandwidth because the link to the remote phone is maintained.

The words **Phone Muted** appear on the top line of the display when outbound audio is muted. The words **Phone Unmuted** appear on the top line of the display when outbound audio is being sent. Outbound audio is always muted when the phone is idle.

NOTE: Outbound audio is always muted when the phone is idle.

4.1.5 Redial

You can quickly redial the last dialed number by pressing **REDIAL**. The redial buffer only remembers the last dialed call, but it does preserve precedence information (see *Changing the Precedence of Your Call* (page 24). Thus, if you dialed a number with high precedence, when you use Redial, the new call will be dialed with the same precedence. The redial buffer is cleared when power is lost or the phone resets (e.g. for 24 hour retest).

4.2 Vertical Services

Some features may be provided by your PBX or local carrier rather than the vIPer phone. This section provides a limited discussion of vertical services. For more information, consult with your carrier or local telecom support department.

4.2.1 Caller ID

Caller ID is one of the most popular services provided. If you use a local carrier, Caller ID must be subscribed to if you want the feature. If you are on a PBX it is probably provided if the PBX has the capability. Received Caller ID information is displayed on the Call Status line.

4.2.2 Call Waiting

Call waiting is another very popular vertical service. It, too, must be subscribed to if you use a local carrier, but is most likely provided by any modern PBX. Call waiting enables a single line phone to handle more than one call by using the infrastructure components (PBX or switch) to place a call on hold and answer or originate a new call, or in some cases to conference calls. Call waiting services are not defined in the NANP and the features provided vary somewhat among carriers and PBXs.

Call waiting service is invoked when you generate a hookflash event. On older analog phones a hookflash was generated by tapping the hookswitch on the handset cradle. That may also work on your vIPer Phone, but it may not work reliably. Depress the **FLASH** key to generate hookflash events to switch between calls.

Typically, a hookflash puts the current call on hold and answers the new call if there is one or allows you to initiate a new call if there is no new inbound call. You may also be able to setup a three-way conference. Your carrier or telecom support department can provide you with the information necessary to use call waiting features.

Typically, call waiting can be canceled on a per-call basis using *70. This feature is commonly used with modems to avoid disruption of a data session. While call waiting should not interfere with operation of PSTN Connect, if you find the phone is occasionally dropping secure calls, try dialing *70 (or other code depending on your telecom service) before you dial a call on which you intend to go secure.

4.2.3 Call Forwarding and Rejection

Call forwarding is the final feature we will discuss in this section. Typical call forwarding features include Call Forwarding which redirects all calls to another phone number, Call Forwarding Busy/No Answer which can be used to redirect the caller to voicemail or a locator service, and Do Not Disturb which plays a “do not disturb” message to the caller. Again, carriers have chosen to implement different call forwarding features and to use different codes to invoke them, so consult with your carrier or telecom support department for information regarding their use.

4.3 Secure Calls

This section guides you through the process of making and terminating secure calls. Before you can do so, however, your vIPer Phone needs to be loaded with key material. Refer to *Load NT1 Keys* (page 55) for further information.

Users of the Sectéra vIPer Phone should consult the *Sectéra vIPer Phone Supplement* for further information on key fill.

4.3.1 Starting a Secure Call

All calls originate as clear calls. Once you have a clear connection, you simply press the **SECURE** key to secure your session.

To establish a clear call, see *Dialing a Call* (page 23).

After you press **SECURE**, you will hear a series of voice prompts indicating the progress of the call. The blue light under the **SECURE** key will blink and then become solid blue when the call is secure. You will also hear a “Line is secure” voice message.

You may receive a **Secure Downgrade** request and hear the voice prompt “Security Downgrade.” When asked, press **Yes** to accept and **No** to abort the Secure Call. If you press **No**, your phone will direct you to press the **CLEAR** key to go Clear. The Security Downgrade prompt occurs for any of the following scenarios:

- Your phone has an APK encryption key and the UnivCert encryption key enabled, but the remote phone only has APK encryption key.
- Both phones have the UnivCert encryption key enabled, but your phone contains Group Key with the Mandatory Exclusion Flag set FALSE and the remote phone does not have the same Group Key.
- Both phones have an APK encryption key, but your phone contains a Group Key with the Mandatory Exclusion Flag set FALSE and the remote phone does not have the same Group Key.

Voice traffic in both directions is muted while the call is going secure. Once the call is secure you can resume your conversation. Also, you will notice some data on the display that indicates your call is secure. You will see **Secure Voice** displayed on the left side and the security level displayed on the right side of the Secure Processor Status Line (see *Figure 3.2-1*). You should also see the “T” Trust Indicator in the left-most column.

> WARNING: If you see a message on the display that indicates you are in a secure call, but the “T” (Trust Indicator) is not present in the first column of the line displaying this data, YOUR CALL IS NOT SECURE and you should not engage in any classified discussion. You should report this problem to your COMSEC Custodian or Security Administrator, as well as to *Customer Support* (page 95).

You should expect three indications that you are in a secure session:

- A solid blue light under the **SECURE** key,
- A voice prompt indicating “Line is secure,” and
- A security level display with a “T” Trust Indicator in the first column of the lines displaying security data.

There may be additional information, but absence of any of the three indications cited above suggests your phone has been compromised and should not be used for secure calls.

Depending upon the device at the other end of your call and network conditions, the vIPer Phone can complete a clear to secure transition in two to twenty seconds. Calls out to the public telephone network will typically take much longer to go secure than calls confined to the Internet.

> *NOTE: The amount of time it takes to go secure may vary, but is generally 15 to 30 seconds.*

There are several reasons why a call can fail to go secure:

- The device on the other end of the call is not compatible. Make sure the device you are calling is SCIP/FNBDT compatible.
- You have incompatible Group Key. See *Group Key* (page 30) for more information.
- Your phone, or the phone at the other end, has not been filled with key material. See *Encryption Key* (page 29) for more information.
- The line quality is insufficient to support a secure call. Hang up and redial; this may result in a better line. Otherwise, consult with your telecom service provider.

NOTE: If the remote party presses **SECURE** *on their phone and you have not yet entered your User ID and PIN, you will immediately receive the "Press* **CLEAR** *to go clear" prompt. This is because your phone is not ready to process secure call setup information. Press* **CLEAR** *and the other party will also be prompted to press* **CLEAR***. Enter your User ID and PIN and try again.*

If you are using a Sectéra vIPer Phone, there are additional reasons why a call might fail to go secure. See the *Sectéra vIPer Phone Supplement* for more information.

4.3.2 Ending a Secure Call

There are two ways to end a secure call:

- Press the **CLEAR** key, or
- Hang up.

If you press **CLEAR**, you should observe the blue light under the **SECURE** key blinking while you hear a series of call progress messages. When you hear "Line is clear" and the blue light is off you can resume your clear conversation. Voice traffic is muted while the call is going clear.

If the other party should press **CLEAR**, you will also be prompted by your phone to press **CLEAR**. This is done to ensure that both parties are aware that the call has returned to a clear session.

If you hang up to end a call, you will not hear voice prompts, but the blue light under the **SECURE** key will turn off.

4.3.3 Secure Call Setup Failures

When you start a secure call, your phone and the remote phone must agree on the parameters (including key material) for the call. If the phones cannot agree, the call fails and the phones revert to clear audio. You are prompted to press **CLEAR** to be sure you are aware that you do not really have a secure session.

The phone will display one of the error messages from *Table 4.3-1* and play "(beep, beep, beep) Secure call failed. Press clear to go clear."

Table 4.3-1: Secure Call Error Messages

Error Message	Description
Modem Error	Your phone was unable to negotiate a digital channel with the phone at the other end. This may be due to low line quality or too much delay in the network. Retry going secure. If that is not successful hang up and try establishing a new call (this may result in the network rerouting your call) or try using a different line. If the problem persists contact your telecom service provider.
No Initiator	The secure call setup signaling has failed. Retry.
No Response	
No Crypto Verify	
Unexpected MID	
Remote Crypto Verification Failed	
Crypto Verification Failed	
Call Setup Timeout	
Reset Timeout	
Transport Error	
No Matching Parameters	Both phones must have common operational mode parameters (e.g., vocoder type). Contact your local Security Administrator.
No Common Operational Mode	Both phones must be configured to support a common operational mode (i.e., secure voice or secure data). For example, this error occurs when your phone calls the remote phone and the remote phone responds in a data mode and your phone is only capable of voice.
No Common Key	The local and remote phones do not have compatible keys. Your phone will not be able to go secure unless both your phone and the remote phone have enabled the UnivCert encryption key or generated an APK encryption key. If Group Keys are present, they must have a matching Group Key. See *Key Management Menu* (page 54) for more information.
No Keys	Your phone needs to have the UnivCert encryption key enabled or an APK encryption key generated. Group Keys cannot be used to make a secure call without the APK encryption key. For additional information, see *Enable UnivCert* (page 56) or *Generate APK* (page 56).
Security Locked	Your phone needs to be unlocked. Enter your Master or User ID and PIN and retry. See PIN Menu (page 50) for more information.
Security Level	This error will occur if you attempt to make a secure call with a remote phone whose minimum Security Level settings do not allow going secure with your APK encryption key. The remote phone must generate an APK key and make sure it's minimum Security Levels are set correctly.

Table 4.3-1: Secure Call Error Messages (continued)

Error Message	Description
Setup Timeout	The secure call setup took too long or the Secure Downgrade prompt was not responded to within one minute, causing the phone to fail the secure call setup. Retry. You may need to extend SCIP Timeout setting if the problem persists. See *SCIP Timeout* (page 67).
Communication Error	The secure connection abruptly terminated. Retry.
Certificate Fail	The secure call setup signaling has failed, retry. If this problem persists, the remote phone does not have a compatible encryption key. Your phone or the remote phone needs to regenerate an APK encryption key. See *View Keys* (page 54).
Group Key Mismatch	Both your phone and the remote phone have a Group Key and the Key Values are not the same. Because the Key Values do not match, the secure call fails. Carefully reload the Group Key into both devices, making sure that the Key Values match.
Remote Communication Timeout	The secure connection cannot be maintained. It may be possible to return to a clear connection by pressing CLEAR.

4.3.4 Secure Dialing

Secure Dial is a means of sending dial digits over a secure connection. For example, suppose you have a secure voice mail server that can be accessed remotely. You would dial the remote access terminal for the secure voice mail server. You then need a means to send dial digits to respond to voice mail prompts provided by the server (e.g., "Press 1 to hear your messages."). Unfortunately, when analog tones are converted to digital, a significant amount of information is removed from the signal, such that the tone decoder at the other end often cannot detect the tone being reproduced by the receiver.

Secure Dial encodes a touch tone signal as a digital message that is then encrypted and sent to the far end. The far end phone then decrypts the message and translates it into the desired tone, distortion free.

You do not need to do anything special to use Secure Dial. Once you go secure, any digits you press are transmitted as Secure Dial digits. The display on the receive end will show the dialed digits, and the tones are reproduced by the handset, headset, or speaker.

You will also be able to give precedence to your Secure Dial number by pressing the **A**, **B**, **C**, or **D** soft keys. See *Changing the Precedence of Your Call* (page 24) for more information on precedence dialing.

4.4 Voice Mail

Voice mail notification may be provided by your carrier or PBX, typically in the form of a stutter dial tone. If you have a message waiting in your voice mail inbox and your carrier or PBX supports message waiting indication, you will hear a series of short dial tones followed by a steady dial tone when you take the phone off-hook. Otherwise, you will hear a steady dial tone.

If you have configured your vIPer Phone's voice mail number, you can access your voice mail server by pressing the **VOICE MAIL** key. See *Voice Mail Number* (page 82) for how to access this setting via the menus. The vIPer Phone is dependent on the capabilities of a voice mail server to provide voice mail support. Your server will provide voice prompts to guide you though listening to messages and personalizing your inbox. Contact your carrier or telecom support department for further information.

Typical voice mail systems do not handle secure voice mail. Should you dial into another vIPer Phone and be directed to a voice mail system, you should not leave any information that you would not want other people to hear, as the voice mail is not stored on the phone, but rather in an unsecured external voice mail recording system. Messages left on the voice mail system may be vulnerable.

WARNING: DO NOT LEAVE CLASSIFIED MESSAGES ON A VOICE MAIL SYSTEM. Your vIPer Phone does not secure messages stored on a voice mail system.

4.5 Headset

A high quality headset, shown in *Figure 4.5-1*, is available as an accessory. The headset should be connected to the "HEAD SET" jack on the left-hand side of your vIPer Phone, seen in *Figure 4.5-2*. Use of the headset is covered in *Audio Device Selection* (page 34).

The headset volume can be adjusted using the volume up/down keys while in a call using the headset.

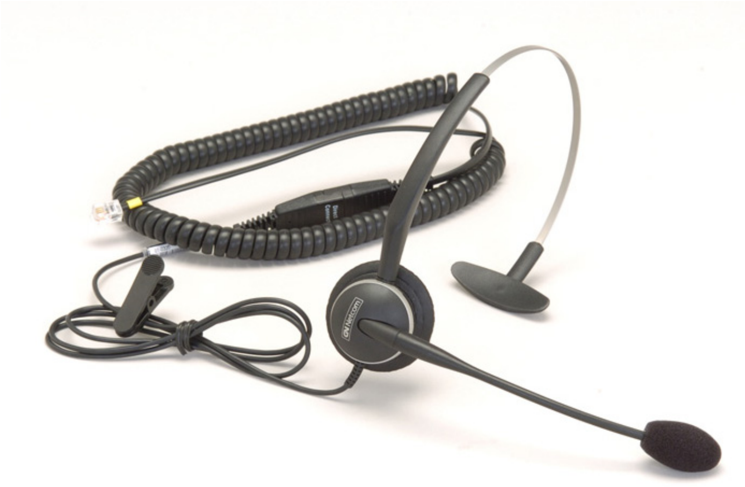


Figure 4.5-1: Headset

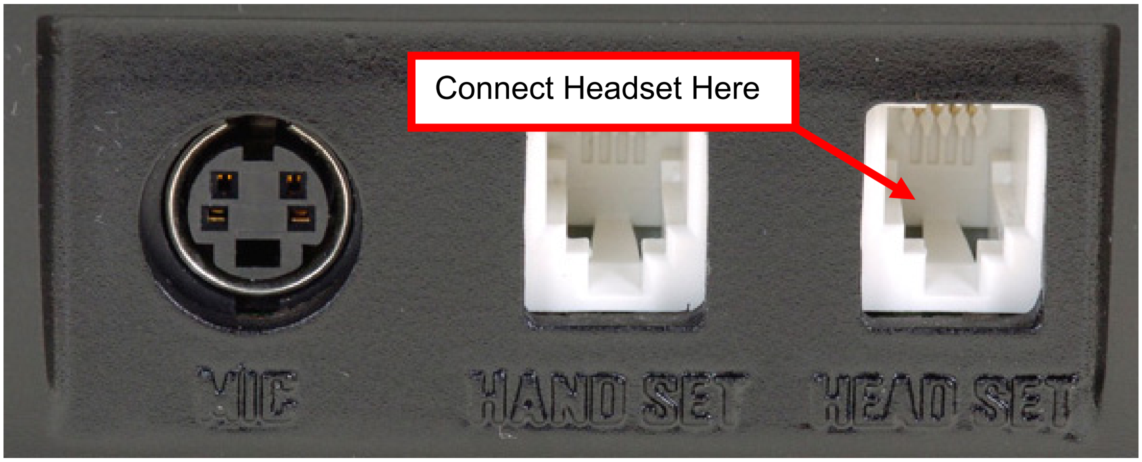


Figure 4.5-2: Headset Connector Location

NOTE: The HEADSET interface of your vIPer Phone has been optimized for use with the accessory headset provided by General Dynamics. Aftermarket headsets are available that may work with your vIPer Phone, but operation is not guaranteed.

NOTE: The MIC interface on your vIPer Phone is currently not used.

4.6 Speakerphone

Your vIPer Phone is provided with built-in speakerphone capability. This section provides information on using the speakerphone to your best advantage.

Use of the speakerphone to originate calls is discussed in *Make a Clear Call* (page 23).

4.6.1 Getting the Best Performance

The internal microphone is optimized for best performance in a high noise environment with a single user. You will get the best performance if you speak directly into the microphone (as opposed to “across” it) located in the lower right-hand corner of the phone.

The microphone will be most sensitive if the phone is placed in the most vertical position on an uncluttered table top. This is because the microphone functions as a “boundary microphone” in which it picks up reflections off the table, as well as the direct sound. In the “flat” position, the microphone does not have the ability to capture reflections off the table. *Figure 4.6-1* illustrates the location of the internal microphone.

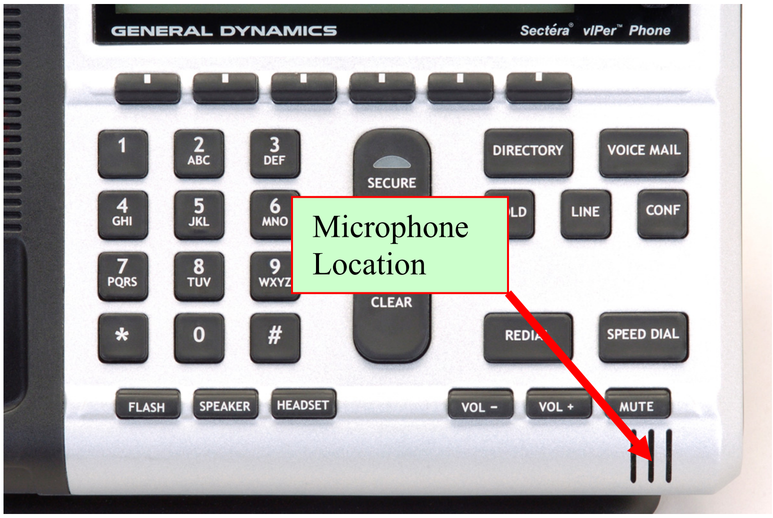


Figure 4.6-1: Microphone Location

If two parties are sharing the speakerphone, the microphone is most effective if you are both in front of the phone speaking directly into it. Alternately, with the phone in the most upright position, a person may be seated to the rear of the phone. Placing persons to either side of the phone is least effective.

4.6.2 External Microphone

The external "MIC" connector on the left-hand side of the phone is not available at this time.

5 Menus

This section discusses the vIPer Phone's menus:

- *Directory Menu* (page 44) accessed by the **DIRECTORY** key
- *Security Menu* (page 50) accessed by the **Security** soft key
- *Phone Settings Menu* (page 80) accessed by the **Phone Settings** soft key

At the beginning of each section you will find a menu path, such as:

DIRECTORY >> Personal Contacts >> Find

The Keystroke Font is used for the word **DIRECTORY**, to indicate that the **DIRECTORY** key is pressed to activate the menu. The Display Font is used for **Personal Contacts** and **Find**, to indicate that these must be selected from the phone's dynamic menus.

The security menu paths are described in tables which are explained in *Security Menu* (page 50).

5.1 Directory Menu

The directory is a compilation of services provided both by your phone and your network consisting of:

- **Speed Dial** – Speed Dial provides the capability to dial frequently used numbers with just two keypresses and to add contacts to the Speed Dial list.
- **Personal Contacts** – Personal Contacts is a local directory maintained by your phone. It can hold up to 200 entries.
- **Inbound Calls** / **Outbound Calls** – The vIPer Phone maintains a record of the last 50 inbound calls and the last 50 outbound calls made and received.

The Directory, shown in *Figure 5.1-1*, is accessed by pressing the **DIRECTORY** key.

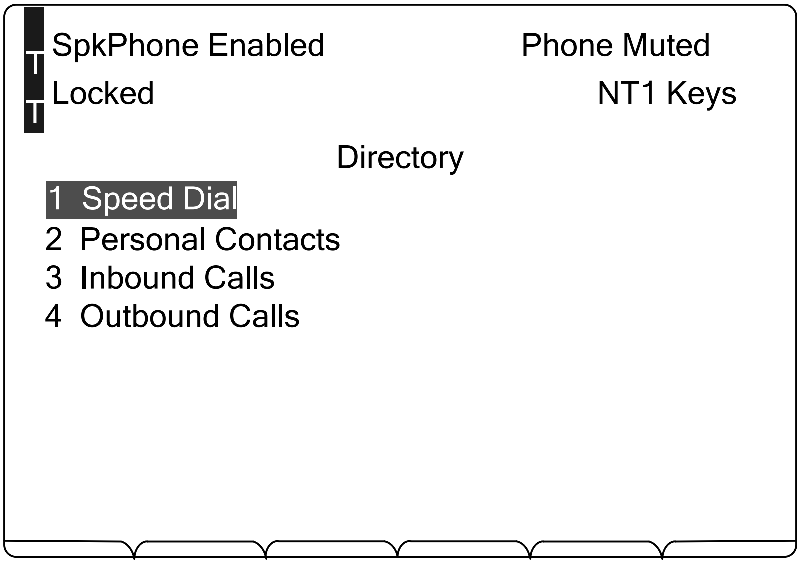


Figure 5.1-1: Directory Menu

5.1.1 Speed Dial

DIRECTORY >> Speed Dial

Your vIPer Phone maintains ten speed dial entries for rapid dialing of frequently used numbers.

5.1.1.1 Adding a Contact to Speed Dial

Before a contact can be added to Speed Dial it first must exist in the Personal Contacts list. Add your contact (see *Adding Contacts*, page 47) if not already in Personal Contacts. If you have already created the contact, use the Search utility (see *Searching Contacts*, page 48) to select the desired contact. With the contact highlighted, press the **Add to Spd Dial** soft key (not the hard key). The phone will display a list of your current Speed Dial contacts. You may select an empty speed dial number, or replace an existing speed dial contact with the new one. Enter the speed dial slot you wish to use (1 through 10) and press **Confirm**.

5.1.1.2 Dialing a Speed Dial Number

Speed Dial contacts are accessed for dialing by pressing the **SPEED DIAL** key or through the Directory menu (**DIRECTORY** >> **Speed Dial**). The phone presents a list of your speed dial contacts, and you can press a number (**1** through **9**, or **0** to access the tenth contact) to dial the number. If the phone is off-hook it will use the handset as the audio device, otherwise it uses the speakerphone. The phone will also dial using the headset if you scroll to the desired contact, then press the **HEADSET** key**.**

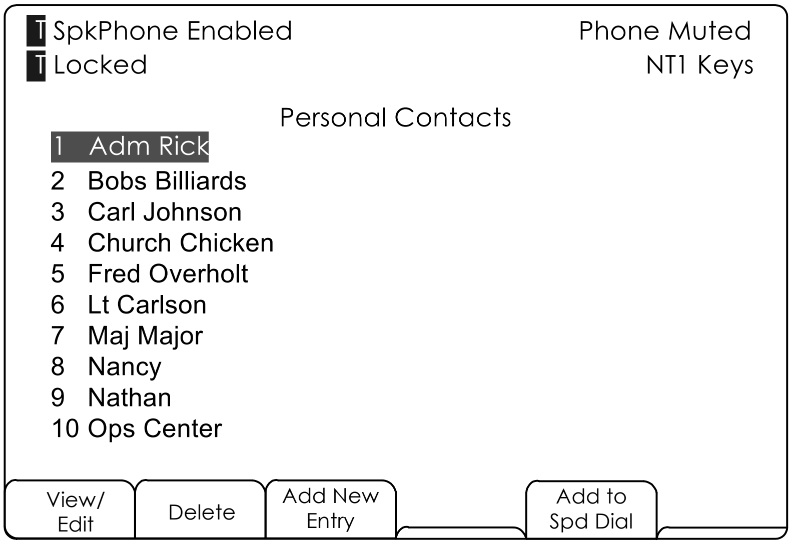
5.1.1.3 Deleting a Speed Dial Number

Scroll to the desired entry and press the **Delete** soft key.

5.1.2 Personal Contacts

DIRECTORY >> Personal Contacts

The Personal Contacts menu is illustrated in *Figure 5.1-2*. The menu functions are provided by soft keys.



T SpkPhone Enabled Phone Muted

T Locked NT1 Keys

Personal Contacts

1 Adm Rick
2 Bobs Billiards
3 Carl Johnson
4 Church Chicken
5 Fred Overholt
6 Lt Carlson
7 Maj Major
8 Nancy
9 Nathan
10 Ops Center

Figure 5.1-2: Personal Contacts

The contacts are displayed ten entries per page. You can scroll through the entries to select the desired contact or use a number key to rapidly select a contact on the displayed page (press **10** to select the tenth entry).

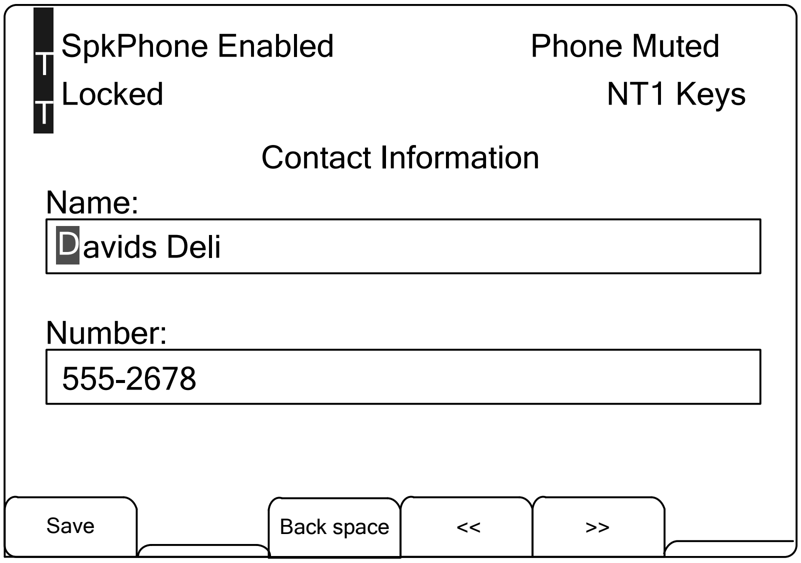
To dial a contact, take the phone off-hook by either

1. lifting the handset,
2. pressing **SPEAKER** or **ENTER**, or
3. pressing **HEADSET**.

The remaining subsections discuss the functions provided by the soft key menus.

5.1.2.1 View/Edit

The **View/Edit** dialog allows you to view and change a contact. Scroll to the contact and press **View/Edit**. You will be presented with the View/Edit dialog, which provides the ability to alter the name and number of the selected contact. The dialog is shown in *Figure 5.1-3*.


SpkPhone Enabled Phone Muted
Locked NT1 Keys

Contact Information

Name: Davids Deli

Number: 555-2678

Figure 5.1-3: View/Edit Dialog

Scroll to the **Name** or **Number** field using the vertical scroll keys. Enter your changes using the dialpad. You can scroll right or left and delete characters using the soft keys. To enter alphabetic characters, rapidly depress the associated number key until the desired character is displayed. The character is accepted when a different key is pressed or you pause 0.5 seconds. Limited punctuation characters are mapped to the **1**, **0**, and * keys (refer to *Table 3.3-1: Key Character Map* on page 20).

Press **Save** to accept your changes, or **EXIT** to back out without making any changes.

5.1.2.2 Deleting Contacts

Scroll to the contact to be deleted and press **Delete**. Press **Yes** in the confirmation dialog.

5.1.2.3 Adding Contacts

You can add a contact to your Personal Contacts list by selecting **Add New Entry** from the **Personal Contacts** menu (*Figure 5.1-2*, on page 46).

The **Add New Entry** dialog is similar to the **View/Edit** dialog, *Figure 5.1-3*, above.

TIP: The scroll keys can navigate between the name and number fields. Pressing **ENTER** saves the contact only if both fields are non-empty. Otherwise, pressing **ENTER** will not save the contact.

TIP: You can also add contacts from your Inbound and Outbound Call Histories and avoid manual entry of some information. See *Adding an Entry to Personal Contacts* (page 49) to find out how.

5.1.2.4 Searching Contacts

Press the **Search** soft key to find a particular entry in the Personal Contacts list. Use the dialpad to enter the first few characters of the name to search for, and press **ENTER** or the **Find** soft key**.** The phone will display the best match to your search, followed by the next nine entries.

5.1.2.5 Adding an Entry to Your Speed Dial List

Scroll or use the Search utility (see *Searching Contacts* on page 48) to select the entry to be added to Speed Dial. With the contact highlighted, press **Add to Spd Dial**. The phone will display a list of your current Speed Dial contacts. You may select an empty speed dial number, or replace an existing speed dial contact with the new one. Enter the speed dial slot you wish to use (1 through 10) and press **Confirm** or **ENTER**.

Alternately you may scroll to the desired slot, press **ENTER**, and **ENTER** again in the confirmation dialog.

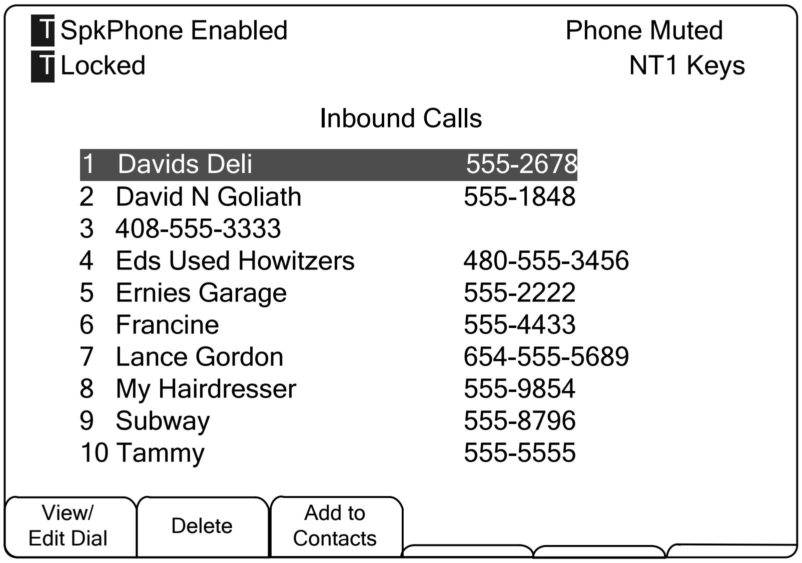
5.1.3 Inbound Calls and Outbound Calls (Call Histories)

DIRECTORY >> Inbound Calls or **DIRECTORY >> Outbound Calls**

Your vIPer Phone maintains a history of the last 50 inbound and outbound calls. You can use the histories to dial callers or populate your Personal Contacts list. Call histories are cleared when the phone loses power or resets (e.g. for 24 hour periodic retest).

5.1.3.1 Inbound and Outbound Histories

The inbound and outbound call histories have a similar format. The Inbound Call history is shown in *Figure 5.1-4*. Select either **Inbound Calls** or **Outbound Calls** from the **Directory** menu.



T SpkPhone Enabled — Phone Muted

T Locked — NT1 Keys

Inbound Calls

1	Davids Deli	555-2678
2	David N Goliath	555-1848
3	408-555-3333	
4	Eds Used Howitzers	480-555-3456
5	Ernies Garage	555-2222
6	Francine	555-4433
7	Lance Gordon	654-555-5689
8	My Hairdresser	555-9854
9	Subway	555-8796
10	Tammy	555-5555

Figure 5.1-4: Call History

5.1.3.2 Dialing from the History

To dial from the call history, do one of the following:

1. Scroll to or enter the number of the desired call and lift the handset (this method uses the handset as the audio device), or
2. Scroll to or enter the number of the desired call and press **ENTER** or **SPEAKER** (this method uses the speakerphone), or
3. Scroll to or enter the number of the desired call and press **HEADSET** to use the headset.

Many networks require you to dial 9 or 8 before dialing an outside number to seize an outside line. You can do that from the call histories using the View/Edit Dial key. Press View/Edit Dial, scroll to the number field, enter the desired prefix digits (you can also select a call precedence – see *Changing the Precedence of Your Call* on page 24) and initiate dialing as described above.

5.1.3.3 Deleting an Entry from a Call History

Delete an entry by scrolling to it and pressing **Delete**. Press **Yes** in the confirmation dialog.

5.1.3.4 Adding an Entry to Personal Contacts

You can add an inbound or outbound call to your Personal Contacts list by scrolling to the call and pressing **Add to Contacts**. The **Add Contact** dialog allows you to edit the entry before committing it to the Personal Contacts. Press **ENTER** to commit the entry, or **EXIT** to abort.

5.2 Security Menu

This section describes the contents of the **Security Menu**. Depending on the Access Control Model chosen when you loaded the first keyset and your user privileges, some of the menu items described in this section may not appear. See *Access Control* (page 26) for more information.

Some menus may require you to enter your PIN, or the Master PIN, before you can access them. This behavior is part of the access control features of the phone and is quite normal. You will not be asked for a PIN if you are not using access controls (Uncontrolled model) or if you entered your PIN previously and the Auto Lock timer has not expired.

Each menu described herein is accompanied by a table that indicates the access control requirements for the menu. For example, *Table 5.2-1* illustrates the access privileges for the Lock Security menu item. The top line indicates the path to the menu, while the next three lines indicate the user types that are allowed to access the menu. Thus, access privileges do not apply under the Uncontrolled model (the menu is not present) while under the Controlled and Restricted models any User (any PIN-holder) can access the menu.

Table 5.2-1: Example Access Control Table

Security >> PIN Menu >> Lock Security Services		
Access Control Model	Uncontrolled	N/A
	Controlled	Any Users
	Restricted	Any Users

The access control table entries are as follows:

- N/A – does not apply for this access control model and the menu is not present.
- PIN User – the individual holding a PIN. No other user can access this menu. For example, only the PIN User can change his PIN. A User cannot change other User's PINs.
- All – anyone.
- Any User – anyone holding a valid PIN, including the Master User.
- Master User – only the Master User (User #1).

Some menus are not visible under all conditions. For example, the Zeroize NT1 menu is only visible when NT1 key (APK key) is present. Other menus are not accessible in the Restricted Access Control Model unless you are the Master User. See *Access Control* (page 26) for more information.

5.2.1 PIN Menu

The **PIN Menu** allows the user to lock the phone's security features and change his security PIN. The PIN Menu will not be visible if you have not created User IDs and PINs.

5.2.1.1 Lock Security Services

The **Lock Security Services** feature allows the user to make the security features of the phone inaccessible until a PIN has been entered. When the security features are locked, a user can place and receive clear calls, access the directory functions, check voice mail, and do other non-security related tasks.

To lock the phone's security features, select **Lock Security Services**. The phone will briefly display **Security Services Locked**. You can unlock the phone by selecting any menu that requires PIN access, or placing a secure call. The phone will prompt you to enter a PIN.

Access privileges for Lock Security are shown in *Table 5.2-2*.

Table 5.2-2: Lock Security Access Privileges

Security >> PIN Menu >> Lock Security Services		
Access Control Model	Uncontrolled	N/A
	Controlled	Any Users
	Restricted	Any Users

5.2.1.2 Change Security PIN

The **Change Security PIN** function allows the current PIN User to change his PIN. The PIN must be 6 digits long. PIN values are not checked for validity other than they must include six digits.

Access privileges for **Change Security PIN** are shown in *Table 5.2-3*.

Table 5.2-3: Change PIN Access Privileges

Security >> PIN Menu >> Change Security PIN		
Access Control Model	Uncontrolled	N/A
	Controlled	PIN User
	Restricted	PIN User

NOTE: Select a PIN that is easy for you to remember. The vIPer Phone will let you enter any sequence of digits you want for a PIN – the only requirement is that it be six digits long. However, certain PINs are not particularly good if you want to prevent unauthorized people from using your phone. For example:
-- Avoid repeating digits or sequential digits.
-- Do not use part of your phone number, driver's license number, or other commonly known number.
-- Do not use recognizable patterns, such as 121212.
Check with your Security Administrator for further guidance on PIN selection.

NOTE: It is not possible for the Master User to change the PINs of other users. If a user forgets his PIN, delete his User ID (via the Zeroize Delete User Menu), and create a new User ID and PIN for him (via the Security Features Add User Menu).

5.2.2 Zeroize Menu

The **Zeroize Menu** allows a user to delete any of the key material loaded into the phone and delete users. The Sectéra vIPer Phone has additional menu items within the Zeroize Menu not discussed in this guide. Sectéra vIPer users should consult the *Sectéra vIPer Phone Supplement* for more information.

5.2.2.1 Zeroize Keyset

Zeroize Keyset is a submenu header for the zeroize functions. Refer to *Table 5.2-4* for the access privileges associated with the zeroize keyset functions.

Table 5.2-4: Zeroize Keyset Access Privileges

Security >> Zeroize >> Zeroize Keyset		
Access Control Model	Uncontrolled	Any User
	Controlled	Any User
	Restricted	Any User

5.2.2.1.1 Zeroize All Keys

Zeroize All Keys deletes all of the key material in the phone. User accounts remain intact. Once you select Zeroize All Keys you will be prompted to confirm the operation. Press **Yes** to confirm and zeroize all keys, or **No** to abort and not zeroize any keys.

When all of the key material has been zeroized the phone cannot be used to place secure calls. Key material must first be reloaded or regenerated.

5.2.2.1.2 Zeroize NT1

Zeroize NT1 is a submenu that contains the APK, UnivCert, and Group key zeroization functions. This menu item is only displayed when UnivCert, APK or Group Keys exist.

5.2.2.1.2.1 Disable UnivCert

Select **Disable UnivCert** to disable use of the Universal Certificate encryption key. You will be presented with a confirmation dialog. Press **Yes** to confirm and disable use of the UnivCert, or **No** to abort and not disable use of the UnivCert encryption key. This menu item will only appear if you have previously enabled the UnivCert encryption key.

5.2.2.1.2.2 Zeroize APK

Select **Zeroize APK** to zeroize the APK encryption key You will be presented with a confirmation dialog. Press **Yes** to confirm and zeroize the APK key pair, or **No** to abort and not zeroize the key pair. This menu item will only appear if you have generated an APK key.

5.2.2.1.2.3 Zeroize Group Key

Zeroize Group Key is a submenu for the Group Key zeroization functions. This menu item will only appear if you have loaded Group Key.

5.2.2.1.2.3.1 Zeroize All Group Key

Select **Zeroize All Group Key** to zeroize all of the Group Keys loaded in the phone. You will still be able to establish secure calls with other phones without a Group Key as long as you have the UnivCert encryption key enabled or have an APK encryption key, but you will not have the added security provided by a Group Key, nor will you have the advantage of exclusion provided by a Group Key.

You will be presented with a confirmation dialog. Press **Yes** to confirm and zeroize all Group Keys, or **No** to abort and not zeroize the Group Keys.

5.2.2.1.2.3.2 Zeroize Group Key Slot

Group Keys are stored in "key slots." One slot is allocated to each key, and the slot used by a key is determined when the key is loaded. The vIPer Phone provides ten group key slots. The **Zeroize Group Key Slot** menu items allow you to select a particular slot to zeroize. Select the slot and press **ENTER**. You will be presented with a confirmation dialog. Press **Yes** to confirm and zeroize the Group Key slot, or **No** to abort and not zeroize the key slot.

When you zeroize a Group Key slot, you lose the ability to establish a secure connection with other holders of that Group Key unless they have at least one Group Key with the Mandatory Exclusion Flag set to False. In this case, they will be asked if they wish to perform a Secure Downgrade to allow a secure connection to be established. See *Key Management Menu* (page 54) for more information.

5.2.2.2 Delete User ID

The **Delete User ID** menu feature allows you to delete any of the users of the phone. If you delete the Master User (User ID #1) while using the Restricted access control model, all functions controlled by the Master User remain inaccessible to all users. To recover these functions you must delete all users, regenerate APK, and reestablish new UserID/PINs.

Access privileges associated with Delete User ID are shown in *Table 5.2-5*.

Table 5.2-5: Delete User ID Access Privileges

Security >> Zeroize >> Delete User		
Access Control Model	Uncontrolled	N/A
	Controlled	Any User
	Restricted	Any User

NOTE: When you delete the last User ID and PIN you will also consequently delete all key material loaded in the phone. You will receive a prompt from the phone when you initiate deleting the last User ID and may choose not to continue at that point. You will have to regenerate APK and reload Group Key if used, before you can make a secure call.

5.2.3 Key Management Menu

The Key Management menu allows you to manipulate the key material stored in your phone. See the *Sectéra vIPer Phone Supplement* for additional information about the keys and cryptology of the Sectéra vIPer Phone.

5.2.3.1 View Keys

The **View Keys** menus allow you to review the status of the various keys stored in the phone.

5.2.3.1.1 View NT1 Key

5.2.3.1.1.1 View UnivCert

The **View UnivCert** menu displays the authentication information in the Universal Certificate. The access privileges for **View UnivCert** are shown in Table 5.2-6.

Table 5.2-6: View UnivCert Access Privileges

Security >> Key Management >> View Keys >> View NT1 Key >> View UnivCert		
Access Control Model	Uncontrolled	All
	Controlled	Any User
	Restricted	Any User

The phone will display the authentication information from the Universal Certificate if UnivCert has been enabled. Otherwise, the phone will display **UnivCert Not Enabled**.

5.2.3.1.1.2 View APK Status

The **View APK Status** menu simply displays whether or not an APK has been generated. The access privileges for View APK Status are shown in *Table 5.2-7*.

Table 5.2-7: View APK Status Access Privileges

Security >> Key Management >> View Keys >> View NT1 Key >> View APK Status		
Access Control Model	Uncontrolled	All
	Controlled	Any User
	Restricted	Any User

The phone will display **APK Keyed** if APK has been generated. Otherwise you will see **APK Not Keyed**.

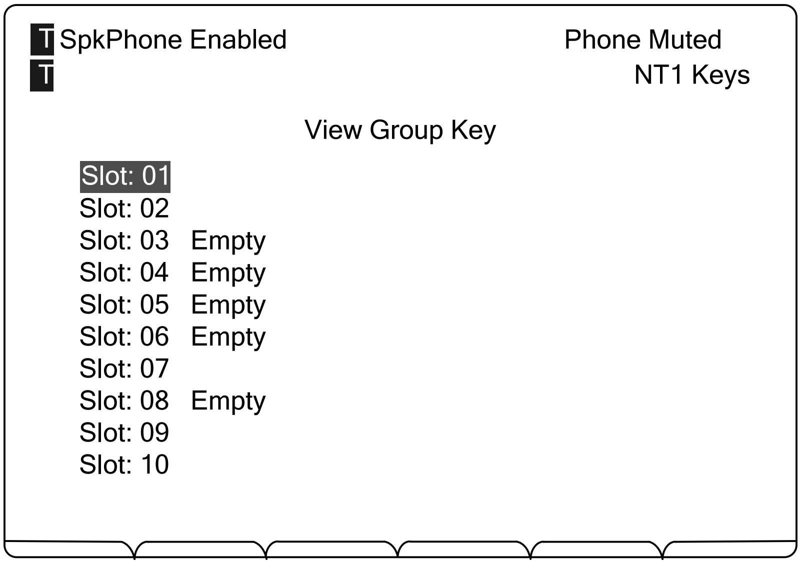
5.2.3.1.1.3 View Group Key

The **View Group Key** menu displays whether or not each of ten Group Key storage slots are loaded. The access privileges for View Group Key are shown in *Table 5.2-8*.

Table 5.2-8: View Group Key Access Privileges

Security >> Key Management >> View Keys >> View NT1 Key >> View Group Key		
Access Control Model	Uncontrolled	All
	Controlled	Any User
	Restricted	Any User

The **View Group Key** display is shown in *Figure 5.2-1*. You can scroll to any of the slots and press **ENTER** to get additional information on the key in that slot. Alternately, you can press a digit (1 – 10) to go immediately to the detail display.



T SpkPhone Enabled Phone Muted
T NT1 Keys

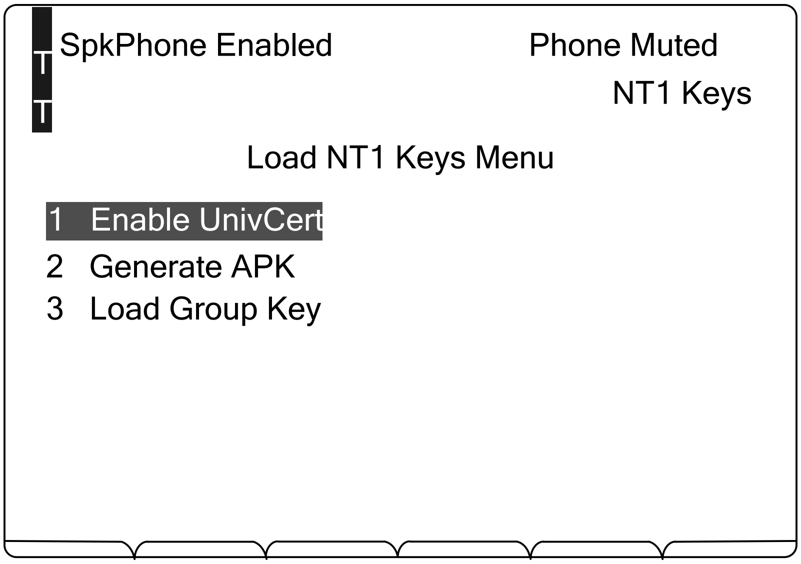
View Group Key

Slot: 01
Slot: 02
Slot: 03 Empty
Slot: 04 Empty
Slot: 05 Empty
Slot: 06 Empty
Slot: 07
Slot: 08 Empty
Slot: 09
Slot: 10

Figure 5.2-1: View Group Key Display

5.2.3.2 Load NT1 Keys

The **Load NT1 Keys** menu is illustrated in *Figure 5.2-2*. Your vIPer Phone is incapable of establishing a secure call until the UnivCert encryption key has been enabled or APK encryption key has been generated. Select either **EnableUnivCert** or **Generate APK** to enable secure call operation.



SpkPhone Enabled Phone Muted

NT1 Keys

Load NT1 Keys Menu

1 Enable UnivCert

2 Generate APK

3 Load Group Key

Figure 5.2-2: Load NT1 Keys Menu

Access privileges associated with the **Load NT1 Keys** menu are shown in *Table 5.2-9*.

Table 5.2-9: Load NT1 Keys Access Privileges

Security >> Key Management >> Load NT1 Keys		
Access Control Model	Uncontrolled	All
	Controlled	Any User
	Restricted	Any User

5.2.3.2.1 Enable UnivCert

The Universal Certificate encryption key must be enabled before it can be used for securing calls. To enable it, select **Enable UnivCert** from the **Load NT1 Keys** menu. You will be guided through the enablement process.

1. Press **Yes** or **ENTER** at the **Enable UnivCert?** prompt.
2. Press **ENTER** to confirm.
3. You will see the **Processing** message.
4. You will see **Key Enable Finished**. Press **ENTER** or **EXIT** to conclude UnivCert key enablement.

See *Access Control* (page 26) for more information about access control models.

5.2.3.2.2 Generate APK

Automatic Public Key is generated by the vIPer Phone. To start generation, select **Generate APK** from the **Load NT1 Keys** menu. You will be guided through the key generation process.

1. Press **Yes** or **ENTER** at the **Begin Generation?** prompt.
2. You will be prompted to press **ENTER** twenty times. Press **ENTER** until the prompt goes away.
3. You will see the **Generating Key Material** message.

4. If this is your first time loading key, or the first time since zeroizing the key, you will be asked to create a user.
5. At the **Add First User?** prompt, press **Yes** to create a User ID and PIN, or **No** if you wish to use the phone without access controls (the Uncontrolled Access Control Model). The process ends if you selected **No**, otherwise continue:
    a. If you pressed **Yes**, you will be prompted to enter a Personal Identification Number (PIN) for User ID 1. A PIN is six digits long and may be any combination of digits you like.
    b. You are then prompted to re-enter the PIN to verify you entered it correctly.
    c. At the **Make User Master**? prompt, press **Yes** if you want the user to be a Master User (which has the effect of choosing the Restricted Access Control Model). Otherwise press **No**, effectively choosing the Controlled Access Control Model.
6. You will see **Add User Successful** followed by **Key Load Finished.** Press **ENTER** or **EXIT** to conclude APK generation.

See *Access Control* (page 26) for more information about access control models.

5.2.3.2.3 Load Group Key

A Group Key is usually generated and loaded using the Group Key Manager Tool. The Group Key Manager Tool and the *Group Key Manager Tool User's Manual* are included on the distribution CD or can be obtained by contacting *Customer Support* (page 95).

5.2.3.2.3.1 Loading Group Key from the Data Port

To load Group Key using the Group Key Manager Tool, select **Load Group Key** from the **Load NT1 Keys** menu, then select **Load Group Key Data Port** and follow the instructions in the *Group Key Manager Tool User's Manual.*

5.2.3.2.3.2 Loading Group Key Manually

A Group Key can also be loaded manually via the dialpad, however it is susceptible to errors and is not recommended unless absolutely necessary. The dialpad operates in alphanumeric mode when manually entering Group Key information. Rapidly depressing or holding down a key will cycle through the alphanumeric characters assigned to the key.

The phone does some checking to ensure that invalid characters are not entered, but there is no integrity mechanism to ensure that the exact same key is entered into all phones. For this reason, manually loading group key should only be considered as a last resort.

To manually load Group Key, select **Load Group Key Keypad** from the **Load NT1 Keys** Load Group Key menu. Select **UnivCert Group/Keypad** to load Group Key associated with calls that use the Universal Cert encryption key, or select **APK Group/Keypad** to load Group Key associated with calls that use the APK encryption key. Then proceed as follows:

1. At the **Enter Slot Number** 1-10 prompt, enter a number 01 through 10 and then press **ENTER**.
2. At the **Short Title:** prompt, enter the Short Title by which the Group Key will be known, up to six characters. A short title is the name of the key that is exchanged during secure call setup. For dialpad entry, the digits 0 through 9 are the only valid characters. Then press **ENTER**.
3. At the **Display ID:** prompt, enter the key name that will be displayed during a secure call, up to sixteen characters. For dialpad entry, the digits 0 through 9 are the only valid characters. Then press **ENTER**.
4. At the **Edition:** prompt, enter the two character edition of the key (1 through 99) and then press **ENTER**.
5. At the **Set Mandatory Exclusion?** Prompt, press **True** or **False**. If you choose False (for *any* Group Key), the phone will be allowed to go secure with other phones not possessing a group key common with one of the group keys in your phone.
6. At the **Key Value Entry** prompt, enter exactly 32 characters, consisting of 0 through 9 and A through F. Use key 2 to enter characters A thru C and key 3 to enter characters D thru F (e.g., 45D202611023CFC991408562DBD827B3).
7. At the **View Group Key?** Prompt, you may choose **Yes** to review the data you entered, or **No** if you are thoroughly confident you entered the data correctly.
8. At the **Key Correct?** prompt, press **Yes** to store the key, or **No** to abort entering the key.
9. If you pressed **Yes**, you will see the **Storing Key** followed by the **Key Load Finished** message.

TIP: A Mandatory Exclusion value of False, in *any* Group Key loaded into your phone, will allow your phone to go secure with *any* phone that does not have a matching Group Key. Mandatory Exclusion values of False should be used with discretion. If you must carry on secure conversations with people who do not use Group Key, you should always set Mandatory Exclusion to False for at least one Group Key.

TIP: If you have a temporary need to go secure with a phone that does not have Group Key, but do not want to allow it normally, enter a bogus Group Key with the Mandatory Exclusion flag set to FALSE, then delete the key when the need for it no longer exists. The key is not actually used, so the values you enter are not important, except for the Exclusion flag.

TIP: If you have a temporary need to go secure with a phone that does not have Group Key, but do not want to allow it normally, enter a bogus Group Key with the Mandatory Exclusion flag set to FALSE, then delete the key when the need for it no longer exists. The key is not actually used, so the values you enter are not important, except for the Exclusion flag.

TIP: When manually entering a key value, it can be tempting to enter something that is easy to enter and remember, such as 12345678901234567890123456789012. While this practice does make entry easy, it does not result in a good key. Good keys should be consist of random data, and random data is neither easy to remember nor enter. General Dynamics recommends, if at all possible, using the Group Key Manager Tool provided on your distribution CD to generate and load your key data. If you are unable to use Group Key Manager to generate your key, there are several good sources of random data on the Internet.

WARNING: Failure to manually enter the same key data used in other phones in the same group will render your phone incapable of going secure with those phones unless Mandatory Exclusion is set to False *for any Group Key*. It is of paramount importance that all key data be entered exactly the same in each phone in a group (except for the Mandatory Flag and the Slot Number). For this reason, Group Key should be manually entered only as a last resort.

NOTE: It is good security practice to distribute key data over a different channel than you use for normal data transfers. For example, do not call a person and recite Group Key data over the phone for which the Group Key is intended, even if the connection is secured. It would be better to mail the data.

5.2.4 Security Features Menu

The Security Features menu addresses the configurable security parameters and some security features of the vIPer Phone.

5.2.4.1 Add User

You can add User IDs and PINs to a vIPer Phone, up to a limit of three. Access privileges associated with Add User are shown in *Table 5.2-10*.

Table 5.2-10: Add User Access Privileges

Security >> Security Features >> Add User		
Access Control Model	Uncontrolled	All
	Controlled	Any User
	Restricted	Master User

To add a user:

1. Select **Add User** from the Security Features Menu.
2. The vIPer Phone will assign a User ID.
3. Enter the PIN for the new user.
4. Press **ENTER**.
5. The display will progress to the next dialog in which you re-enter the PIN.
6. Press **ENTER** again.
7. If this is the first User ID/PIN created, you will see the **Make User Master?** prompt. Press **Yes** if you want a Master User; **No** otherwise.

See *Access Control* (page 26) for more information on access control models and why you might want to create a Master User.

> *NOTE: Creating a Master User has the effect of hiding the* **Security Features Menu** *from the other, non-Master users.*

5.2.4.2 Delete User

You can delete Users from a vIPer Phone to revoke access to the security features of the phone. Access privileges associated with Delete User are shown in *Table 5.2-11*.

Table 5.2-11: Delete User Access Privileges

Security >> Security Features >> Delete User		
Access Control Model	Uncontrolled	N/A
	Controlled	Any User
	Restricted	Master User

To delete a user:

1. Select **Delete User** from the Security Features menu.
2. Enter a User ID (1, 2, or 3 are valid choices) at the **Delete User ID** prompt.
3. Press **ENTER**.
4. You will receive a confirmation prompt – **Do you really want to delete user n?** Press **Yes** to confirm, **No** to abort.

Once a User ID and PIN are deleted, the holder of that User ID will not be able to access the security features of the phone.

WARNING: If you delete a Master User, the **Security Features Menu** will be inaccessible until all User IDs are deleted.

WARNING: If you delete the last User, all key material in the phone will also be deleted.

5.2.4.3 Auto Lock

The Auto Lock function locks the phone's security features after a prescribed period of non-security use.

Table 5.2-12: Auto Lock Access Privileges

Security >> Security Features >> Auto Lock		
Access Control Model	Uncontrolled	N/A
	Controlled	Any User
	Restricted	Master User

This menu is not available until a PIN is created. You can activate or deactivate the Auto Lock feature through the Auto Lock menu, shown in *Figure 5.2-3*. Once the security features are locked, you must re-enter a valid PIN to enable them again.

Select **ON** to enable the Auto Lock feature, or **OFF** to disable the feature. The "**>**" indicates the active selection. If you select **ON**, you will be prompted to enter an Auto Lock timeout, shown in *Figure 5.2-4*. Enter a timeout ranging from 01 to 99 minutes. If you enter 00, the phone will display **Value Invalid** and use the previously defined value.

The Auto Lock timer is reset and restarted each time you exit a security feature menu or end a secure call. As long as you are in a secure call, or are accessing a security feature menu, the timer has no effect. The Auto Lock feature will not interrupt a secure call. Once you end the secure session, the timer will restart.

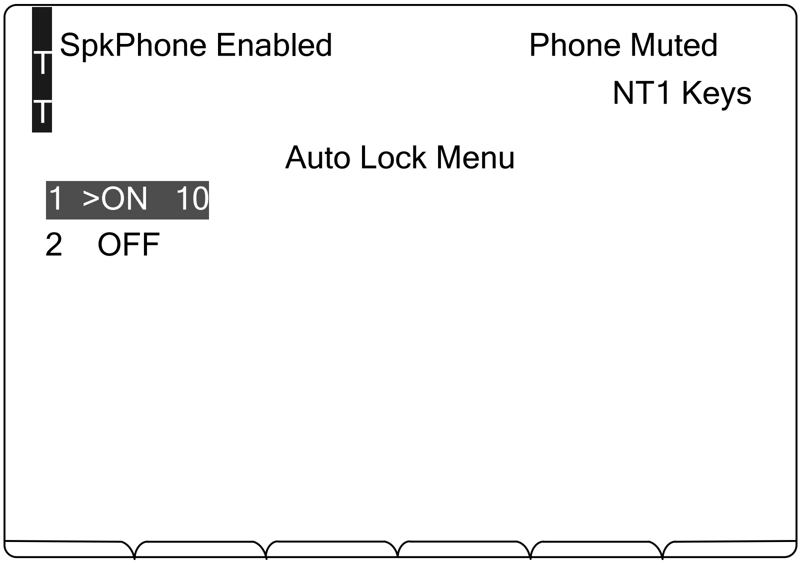


Figure 5.2-3: Auto Lock Menu

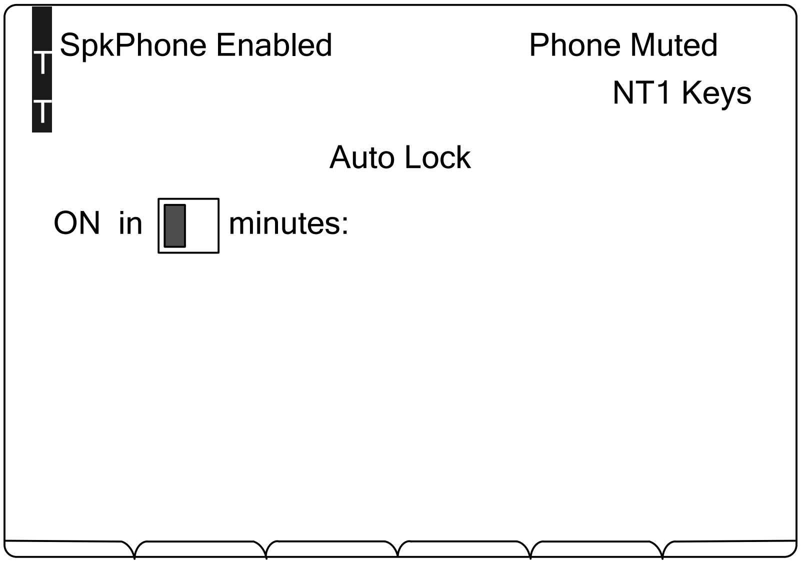


Figure 5.2-4: Auto Lock Timeout Dialog

5.2.4.4 Application Control

The Application Control menu item currently contains only one item used to control the Auto Secure on Answer feature.

When Auto Secure on Answer is enabled, your phone will automatically attempt to go secure when you answer an incoming call. If unable to go secure, your phone will prompt you to press the **CLEAR** key to enter a clear voice call. The active selection is shown by the "**>**" symbol.

Access privileges for Application Control are shown in *Table 5.2-13*.

Table 5.2-13: Application Control Access Privileges

Security >> Security Features >> Application Control		
Access Control Model	Uncontrolled	All
	Controlled	Any User
	Restricted	Master User

5.2.4.5 Security Level

The Security Level menu item is used to limit secure operation by specifying a minimum and maximum security level authorized for secure calls.

> *NOTE: The security levels increase in order from SECURE APK (lowest) to PROTECTED (highest).*

You can use the minimum and maximum security levels to limit secure operation. For example, by setting the minimum and maximum level to PROTECTED, a vIPer Phone that has UnivCert encryption key enabled and APK encryption key generated will only be able to establish a secure call with terminals with UnivCert encryption key enabled, prohibiting all APK secure calls. The default minimum security level is SECURE APK, and the default maximum security level is PROTECTED.

> *NOTE: Use this feature carefully as secure operation can be prohibited. Here are some examples: 1) Setting the minimum level to PROTECTED (for UnivCert encryption key) will prohibit APK secure operation. 2) Setting the maximum level to SECURE APK (for APK encryption key) will prohibit UnivCert secure operation.*

Access privileges for Security Level are shown in *Table 5.2-13*.

Table 5.2-14: Security Level Access Privileges

Security >> Security Features >> Security Level		
Access Control Model	Uncontrolled	All
	Controlled	Any User
	Restricted	Master User

To change the security level settings:

1. Select **Security Level**from the Security Features Menu.
2. The vIPer Phone will prompt for the **Min Voice Level**.
3. Scroll or use the number keys to select between PROTECTED and SECURE APK.
4. The vIPer Phone will prompt for the **Max Voice Level**.
5. Scroll or use the number keys to select between PROTECTED and SECURE APK.

6. The vIPer Phone will notify you if you have selected settings that prohibit secure voice based on your currently loaded keys; otherwise, the vIPer Phone will return to the Security Features Menu.

5.2.4.6 Speakerphone

Certain environments may require disabling the Speakerphone. Navigate to the **Speakerphone** menu and select **Disabled** to prevent use of the Speakerphone. The active selection is shown by the "**>**" symbol. You can also verify the setting of the **Speakerphone** feature on the top line of the display.

Access privileges associated with the speakerphone control are shown in *Table 5.2-15*.

Table 5.2-15: Speakerphone Control Access Privileges

Security >> Security Features >> Speakerphone		
Access Control Model	Uncontrolled	All
	Controlled	Any User
	Restricted	Master User

5.2.4.7 Black Computer Port

The Black Computer Port is labeled 10/100 PC on the vIPer Phone and is disabled by the PSTN Connect software. It cannot be used in the PSTN Connect configuration. While the setting can be changed it has no effect on the port in PSTN mode.

5.2.4.8 Web Interface

In PSTN operation this feature is disabled unless the network processor software is being upgraded. It cannot be used in normal operation. While the setting can be changed it has no effect in normal PSTN operation. If you change the setting the phone will reset, but the web interface will still be inactive, regardless of the setting.

Refer to Section 6, *Updating Network Software*, on page 83 for more information.

5.2.4.9 CLR Event Buffer

The vIPer Phone maintains a record of security events and system errors that occur during operation. This buffer is circular in nature in that once it fills up it begins overwriting the oldest records. Occasionally, when debugging problems with the phone, it is necessary to clear this buffer to ensure that you get fresh data. Normally you will only need to do this when *Customer Support* (page 95) is helping you debug a problem. To clear the buffer, select **CLR Event Buffer** and press **Yes** in the confirmation dialog.

Table 5.2-16: CLR Event Buffer Access Privileges

Security >> Security Features >> CLR Event Buffer		
Access Control Model	Uncontrolled	All
	Controlled	Any User
	Restricted	Master User

5.2.5 Service Menu

The Service Menu contains various submenus that provide information related to the operational condition of the vIPer Phone. All submenus carry the same access privileges, illustrated in *Table 5.2-17*.

Table 5.2-17: Verify Software Access Privileges

Security Menu >> Service Menu		
Access Control Model	Uncontrolled	All
	Controlled	Any User
	Restricted	Any User

5.2.5.1 Verify Software

Verify Software can be used to verify the cryptographic integrity of the software loaded in your phone. Some organizations may require users to run this feature periodically to ensure the software has not been tampered with. Select **Verify Software** from the **Service Menu** and wait for completion. You will see the **Verifying Software Please Wait** message while the phone checks internal signatures on its software load. When the check is completed you will either see **Software Verify Successful** or **Software Verify Failed**. You should contact your security officer for further instructions if the verification fails.

NOTE: The Verify Software function only checks the security software. It does not verify the integrity of the networking software. The networking software and the clear vocoder are checked each time the phone is powered on and during a 24-hour retest; however this check is not as rigorous as that performed on the security software by the Verify Software function.

5.2.5.2 System Retest

System Retest has the same effect as removing and reapplying power to the phone. Select **System Retest** from the **Service Menu** if you are experiencing problems with the phone. The **Perform System Retest?** message will appear. Press **ENTER** to confirm. See *If You Have Problems* (page 86) for additional information.

5.2.5.3 Event Buffer

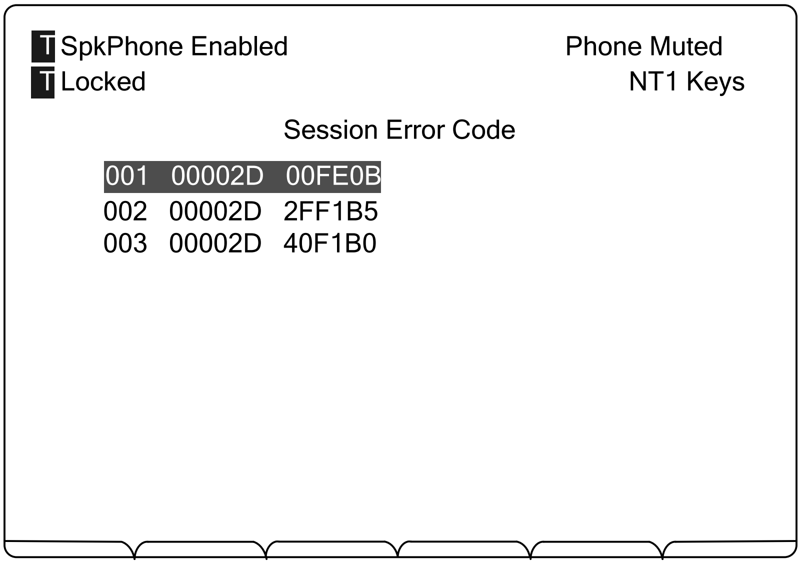
The Event Buffer allows you to view error and status codes stored by your phone.

- Error Codes are recorded when something goes wrong. Error Codes typically indicate malfunctions of the phone.
- Status Codes are recorded during normal operation of the phone.

The Event Buffer is an important troubleshooting tool but should not normally be needed. If you call *Customer Support* (page 95) they may request a copy of the event buffer. See *If You Have Problems* (page 86) for additional information.

5.2.5.3.1 View Error Code

Select **View Error Code** to retrieve a list of the error codes recorded by your phone. A sample Error Code list is shown in *Figure 5.2-5*. The first column of numbers is simply a reference number. The second column is the session number, and the third column is the Error Code.



```
T SpkPhone Enabled                      Phone Muted
T Locked                                   NT1 Keys
                Session Error Code
     001  00002D  00FE0B
     002  00002D  2FF1B5
     003  00002D  40F1B0
```

Figure 5.2-5: Error Code List

You can scroll through long lists with the vertical scroll keys.

5.2.5.3.2 View Status Code

Select **View Status Code** to retrieve a list of the status codes recorded by your phone. The Status Code list is very similar to the Error Code list shown in *Figure 5.2-5*. The first column of numbers is simply a reference number. The second column is the session number, and the third column is the Status Code.

5.2.5.4 Version Info

Version Info allows you to view the software version numbers of the various applications residing in the phone. Select this item to view the following information:

- SCP Boot Ver: The Secure Call Processor boot software version number
- SCP Oper Ver: The Secure Call Processor operational software version number
- Secure VP Boot Ver: The Secure Vocoder boot software version number
- Secure VP Oper Ver: The Secure Vocoder operational software version number
- FPGA Ver: The security firmware version number
- Network Proc Boot Ver: The Network Processor boot software version number

- Network Proc Oper Ver: The Network Processor operational software version number
- Network Proc Cure Ver: The **N**etwork **C**ode **U**pgrade **Re**covery software version number
- HMI Boot Ver: The HMI Controller boot software version number
- HMI Oper Ver: The HMI Controller operational software version number

The above information is useful if you must report a problem to *Customer Support* (page 95).

5.2.5.5 Terminal Serial Number

Select **Terminal Serial Number** to view the electronic serial number of your phone. This version number should match the version number on the product label.

5.2.6 Configuration Menu

The Configuration Menu allows you to change some of the parameters affecting the secure operation of the phone. Access privileges for the sub-menus within the Configuration Menu are shown in *Table 5.2-18*.

Table 5.2-18: Configuration Menu Access Privileges

Security >> Configuration Menu		
Access Control Model	Uncontrolled	All
	Controlled	Any User
	Restricted	Any User

5.2.6.1 View Fill Status

The **View Fill Status** menu shows you what type of keys the phone has loaded. It does not tell you anything about the keys, however. For more detailed information, navigate to **Security** >> **Key Management** >> **View Keys** (limited to Master User if you are using the Restricted Access Control Model (see *Access Control* on page 26).

5.2.6.2 Network Settings

The **Network Settings** menu displays network settings related to secure sessions only.

5.2.6.2.1 SCIP Timeout

The SCIP timeout is a secure call setup timeout that normally should not need to be changed. If your network experiences long delays and calls fail to go secure, it may be beneficial to experiment with a longer timeout value.

NOTE: Changing SCIP timeouts will have no effect on clear call performance. Contact your telecom service provider if you are experiencing performance problems with clear calls.

5.2.6.3 Red Data Port

The **Red Data Port** menu allows you to configure the Red Data Port. The Red Data Port is a shared port, providing both a standard DB-9 RS-232 connector and a B style USB connector. The Red Data Port is located on the back of the vIPer Phone and is labeled **SECURE DATA/FILL**.

The vIPer Phone does not support secure data at this time. The Red Data Port can be used for accessing and configuring certain features of the phone, but cannot be used for transmitting secure data. A software update will be provided when additional Red Data support is available. Refer to *Updating Security Software* (page 84) for instructions related to updating this software.

NOTE: The Red Data Port will automatically switch between USB and RS-232 based on what is connected. Both USB and RS-232 cannot be used simultaneously. If you have been using one port, then need to use the other, it may be necessary to remove and reapply power, or execute the Service Menu System Retest function (see System Retest on page 65).

5.2.6.3.1 USB Red Data Port Driver Installation and Use

The USB Red Data Port Driver is included on your distribution CD and can also be obtained by contacting *Customer Support* (page 95). This driver must be installed on your computer before you can use the USB Red Data Port.

The USB Red Data Port driver creates a virtual COM port on your computer and generally assigns the next highest COM port to the USB Red Data Port. For example, if you have a computer with no modem, it will create COM3 and assign it to the USB Red Data Port. If you have a computer with a modem, it will create COM4 and assign it to the USB Red Data Port.

5.2.6.3.1.1 Installing the USB Red Data Port Driver

To install the USB Red Data Port Driver on your computer and connect your computer to the USB Red Data Port, follow these steps:

1. Insert the distribution CD into your CD drive. Open the **Utilities Folder** and then the **USB Red Data Port Driver** Folder.
2. Double click on **PreInstaller.exe**. The **Install Driver** window will appear. Click on **Install**. You will see **Installation Successful**.
3. Plug one end of the USB cable into the **SECURE DATA/FILL** USB port on the back of the vIPer Phone and the other end into the USB port on your computer.
4. The **Welcome to the Found New Hardware Wizard** window will appear.
5. Click on **No, not this time** and then click **Next**.
6. Click on **Install from a list or specific location (Advanced)** and then click **Next.**
7. Click on **Search removable media (floppy, CD-ROM…)** and click **Next**.
8. The **Completing the Found New Hardware Wizard** window will appear and will say "The wizard has finished installing the software for CP210x USB Composite Device". Click **Finish**.
9. You have successfully setup the USB. Now repeat steps 4 through 7 to setup the COM bridge
10. The **Completing the Found New Hardware Wizard** window will appear and will say "The wizard has finished installing the software for CP210x USB to UART Bridge Controller". Click **Finish**.
11. The **Found New Hardware** balloon will appear in bottom right corner of your computer screen and say "Your new hardware is installed and ready to use".

After the driver is installed, you can use the USB Port of your computer with any serial communication application to control the vIPer Phone (e.g. send AT commands or perform a security software update). To verify that the USB Red Data Port has been successfully installed, see *Creating a Basic HyperTerminal Session* below.

5.2.6.3.1.2 Creating a Basic HyperTerminal Session

To communicate with your vIPer Phone using HyperTerminal, follow these steps:

1. On your vIPer Phone, press the **Security** soft key and then set the Configuration Menu->Red Data Port->Data Port Rate to **9600**.
2. On your computer, click **Start**, located in the lower left-hand corner.
3. Click **Programs**.
4. Click **Accessories**.
5. Click **Communications**.
6. Click **HyperTerminal.** A HyperTerminal window will appear.
7. Enter a descriptive name, select an appropriate icon, and click **OK**.
8. Select the COM Port you wish to use from the pull down menu next to "**Connect using:**" and then click **OK**.
9. Select the following and then click **OK**: Bits per second: **9600**, Data bits: **8**, Parity: **None**, Stop bits: **1** and Flow control: **Hardware**

10. On the HyperTerminal screen, type “**AT**”, press **ENTER**, and verify that “**OK**” is displayed. You should see information similar to this displayed on the HyperTerminal bottom bar: “**Connected: 00:00:07 Auto detect 115200 8-N-1**”. Once this occurs, you have a working HyperTerminal session. This proves that the USB Red Data Port is working.
11. The most common errors that have occurred if you get no “**OK**” response are that the baud rate is set incorrectly or the wrong COM Port has been selected. If you are unable to see the text you typed or if you get a “**0**” response, type “**ATE1V1**” and press **ENTER**. Then type “**AT**”, press **ENTER,** and verify that “**OK**” is displayed.

5.2.6.3.1.3 Uninstalling the USB Red Data Port Driver

If you have any problems using the USB Red Data Port Driver, remove and reinstall the driver. To uninstall the USB Red Data Port Driver, follow these steps:

1. Access the **Control Panel** on your computer.
2. Select **Add or Remove Programs**.
3. Select **CP210x USB to UART Bridge Controller**.
4. Select **Change/Remove**.

To reinstall the driver (see *Installing the USB Red Data Port Driver* on page 69). If you continue to have problems, contact *Customer Support* on page 95 for assistance.

5.2.6.3.2 Data Port Rate

The Data Port Rate menu allows you to set the operating rate (Baud rate) of the RS-232 port. It has no effect on the USB port.

The RS-232 port is configured for 1 start bit, 1 stop bit, and no parity. These settings cannot be changed.

Scroll to the desired rate and press **ENTER** to select it. Supported rates are 2400, 4800, 9600, 14400, and 115200 baud. The active selection is indicated by the “**>**” symbol.

NOTE: The data port rate should match the rate supported by the computer connected to the Red Data Port.

5.2.6.3.3 Data Port Mode

The Data Port Mode Menu selects the operating mode for the RS-232 port. It has no effect on the USB port.

The Data Port Mode is only used to update security software, send AT commands, and other administrative functions. Data Port Mode should be left in the Normal mode. The Data Port Mode feature allows you to select one of the following operational modes:

Normal:

- Use this setting for most scenarios.
- In this mode, the DATA Port interface signals are always enabled.
- When DTR is asserted, the phone recognizes that a data device is attached to its DATA Port and ready to use.

Ignore DTR:

- Use this setting when you want to:
    - use a non-standard Host Computer that does not provide the DTR signal.

Power Save:

- Use this setting for low power mode (i.e., when powered by a battery).
- In this mode, the signals on the DATA Port Interface are disabled unless DTR from your Host Computer is asserted.
- Once DTR is asserted, there is no difference between Normal and Power Save modes.

Scroll to the desired operating mode and press **ENTER** to select it. In general, the mode setting should be left as **Normal**, unless that setting does not work. The active selection is indicated by the "**>**" symbol.

5.2.6.3.4 AT Command Support

Table 5.2-19 describes the AT commands supported by your phone for use in remote control situations. AT commands can be sent to the phone via the Red Data Port or Red USB Port using a terminal emulation program. If you get an error response when you enter an AT command, see *Table 5.2-23: AT Command Error Codes* on page 79 for the error description.

Table 5.2-19: AT Commands

AT Command	Data Format	Function	Response
ATI10	none	Report Product TSN (Terminal Serial Number)	I10:<TSN>
ATI11	none	Report Version Number	I11:<versions>[3]
ATV	0 = terse 1 = verbose	Result Code Form	OK or ERROR
AT~CD	0 = Personal Contacts (default) 1 = Inbound Calls 2 = Outbound Calls 3 = Speed Dial	Deletes all entries in the specified directory.	OK or ERROR
AT~CR	none	Boot Crash Recovery – forces network processor into CURE on next power cycle	OK
AT~DA	none	Clear Status Buffer	OK
AT~DB	none	Report Status Buffer	Variable length buffer contents
AT~DD	none	Request Display Lines	Variable length text
AT~DE	none	Network Status	Variable length text
AT~DF	none	Battery Status	Variable length text
AT~DG	none	Power On Self Test (POST) Status	Variable length text
AT~FA	none	Request Far-end Authentication	Variable length text
AT~FH	variable length code per *Table 5.2-22*	Set Straps	OK or ERROR
AT~FK	2-digit code per *Table 5.2-20*	Remote Keypress	OK or ERROR, depending on code

[3] Versions consists of a concatenation of processor versions in the format "MMMMmmmmbbbb" where MMMM is the major version, mmmm is the minor version, and bbbb is the build number. The order of versions is: SCP Boot, SCP Oper, VP Boot, VP Oper, FPGA, Network Proc Boot, Network Proc Oper, Network Proc Cure, HMI Boot, HMI Oper.

Table 5.2-19: AT Commands (continued)

AT Command	Data Format	Function	Response
AT~FMK	Octets 0-1 see *Table 5.2-20*, octets 2-3 keypress count, range 01 to 99	Multiple Remote Keypress – effectively actuates a keypress from 1 to 99 times. Example: AT~FMK1402 presses the **EXIT** key two times.	OK or ERROR depending on code
AT~FX	none	System Retest	OK
AT~FZ	A = all	Zeroize all Keys and User IDs	OK or ERROR
AT~FZ	C	Zeroize Confirmation. Must be sent immediately after AT~FZ above to confirm zeroize request.	OK
AT+GCI	2-digit code per *Table 5.2-21*	Set the country code for the PSTN Connect accessory	OK
AT+GCI?	none	Query which country code is set for the PSTN Connect accessory	2-digit code per *Table 5.2-21*
AT~TE	0,x where x = 0 – off 1 – low 2 – low/mid 3 – mid 4 – high/mid 5 – high	Backlight Control Example: AT~TE0,3 sets backlight to mid	OK or ERROR
AT~TF	xx, where xx is in the range 00 (lowest) to 11 (highest)	Contrast Control	OK or ERROR

Table 5.2-20: Keypress Codes

Code	Key	Code	Key	Code	Key
00	0	11	**CLEAR**	20	**SPEAKER**
01	1	12	Scroll down	21	**HEADSET**
02	2	13	**ENTER**	20	**SPEAKER**
03	3	14	**EXIT**	21	**HEADSET**
04	4	15	Scroll Up	22	**REDIAL**
05	5	16	**MODE**	23	**DIRECTORY**
06	6	17	Soft key 1	24	**CONFERENCE**
07	7	18	Soft key 2	25	**SPEED DIAL**
08	8	19	Soft key 3	26	**VOICE MAIL**
09	9	1A	Soft key 4	27	**FLASH**
0A	*	1B	Soft key 5	28	**HOLD**

Table 5.2-20: Keypress Codes (continued)

Code	Key	Code	Key	Code	Key
0B	#	1C	Soft key 6	29	**LINE**
10	**SECURE**	1D	**MUTE**	Other	Responds with Error

Table 5.2-21: Country Codes

Country	Code	Country	Code	Country	Code
Afghanistan	5C	Lesotho	65	Kyrgyzstan	CA
Albania	01	Liberia	66	Laos	63
Algeria	02	Libya	67	Latvia	F8
American Samoa	03	Liechtenstein	68	Norway	82
Andorra	E7	Lithuania	F7	Oman	83
Angola	43	Luxembourg	69	Pakistan	84
Anguilla	05	Macao	6A	Palau	D7
Antigua & Barbuda	06	Macedonia	E4	Panama	85
Argentina	07	Madagascar	6B	Papua New Guinea	86
Aruba	EE	Malawi	6D	Paraguay	87
Ascension	08	Malaysia	6C	Peru	88
Ascension Island	F3	Maldives	6E	Philippines	89
Australia	09	Mali	6F	Poland	8A
Austria	0A	Malta	70	Portugal	8B
Azerbaijan	C8	Marshall Islands	D3	Puerto Rico	8C
Bahamas	0B	Martinique	DE	Qatar	8D
Bahrain	0C	Mauritania	71	Reunion Island	F2
Bangladesh	0D	Mauritius	72	Romania	8E
Barbados	0E	Mayotte	F0	Russian Federation	B8
Belarus	1E	Mexico	73	Rwanda	8F
Belgium	0F	Micronesia Federated States	D4	Saint Croix	91
Belize	10	Moldova	E8	Saint Helena and Ascension	92
Benin	11	Monaco	74	Saint Kitts & Nevis	90
Bermuda	12	Mongolia	75	Saint Lucia	93
Bhutan	13	Montserrat	76	Saint Pierre & Miquelon	E3
Bolivia	14	Morocco	77	Saint Thomas	95
Bosnia & Herzegovina	E5	Mozambique	78	Saint Vincent & the Grenadines	97

Table 5.2-21: Country Codes (continued)

Country	Code	Country	Code	Country	Code
Botswana	15	Myanmar (Burma)	1C	Samoa	BE
Brazil	16	Namibia	F1	San Marino	94
British Antartic Territory	17	Nauru	79	Sao Tome & Principe	96
British Indian Ocean Territory	18	Nepal	7A	Saudi Arabia	98
British Virgin Islands	19	Netherlands	7B	Senegal	99
Brunei Darussalam	1A	Netherlands Antilles	7C	Serbia	C1
Bulgaria	1B	New Caledonia	7D	Seychelles	9A
Burkina Faso	B6	New Zealand	7E	Sierra Leone	9B
Burundi	1D	Nicaragua	7F	Singapore	9C
Cambodia	2F	Niger	80	Slovakia	C5
Cameroon	1F	Nigeria	81	Slovakia	FB
Canada	20	Niue	D6	Slovenia	FC
Cape Verde	21	Norfolk Island	D8	Solomon Islands	9D
Cayman Islands	22	French Polynesia	3E	Somalia	9E
Central African Republic	23	Gabon	40	South Africa	9F
Chad	24	Gambia	41	Spain	A0
Chile	25	Georgia	C9	Sri Lanka	A1
China	26	Germany	04	Suriname	A3
Christmas Island	D9	Germany	42	Swaziland	A4
Cocos Keeling Islands	DD	Ghana	44	Sweden	A5
Columbia	27	Gibraltar	45	Switzerland	A6
Comoros	28	Greece	46	Taiwan	FE
Congo	29	Greenland	EC	Tajikistan	D1
Cook Islands	2A	Grenada	47	Tanzania	A8
Costa Rica	2B	Guadeloupe	E1	TBR21	FD
Cote D'Ivoire	5A	Guam	48	Thailand	A9
Croatia	FA	Guatemala	49	Togo	AA
Cuba	2C	Guernsey	4A	Tokelau	D5
Cyprus	2D	Guinea	4B	Tonga	AB
Czech Republic	2E	Guinea Bissau	4C	Trinidad & Tobago	AC
Dem. Rep. of the Congo	C2	Guyana	4D	Tunisia	AD
Denmark	31	Haiti	4E	Turkey	AE
Diego Garcia	F4	Honduras	4F	Turkmenistan	C7

Table 5.2-21: Country Codes (continued)

Country	Code	Country	Code	Country	Code
Djibouti	32	Hong Kong	50	Turks and Caicos Islands	AF
Dominica	34	Hungary	51	Tuvalu	B0
Dominican Republic	33	Iceland	52	Uganda	B1
East Timor	E6	India	53	Ukraine	B2
Ecuador	35	Indonesia	54	United Arab Emirates	B3
Egypt	36	Iran	55	United Kingdom	B4
El Salvador	37	Iraq	56	United States	B5 (Default)
Equatorial Guinea	38	Ireland	57	Uruguay	B7
Eritrea	EF	Israel	58	US Virgin Islands	F5
Estonia	F9	Italy	59	Uzbekistan	EB
Ethiopia	39	Jamaica	5B	Vanuatu	B9
Falkland Islands	3A	Japan	00	Vatican City	BA
Faroe Islands	ED	Jersey	5D	Venezuela	BB
Fiji	3B	Jordan	5E	Vietnam	BC
Finland	3C	Kazakhstan	D2	Wallis & Futuna	BD
France	3D	Kenya	5F	Yemen	BF
French Antilles	E0	Kiribati	60	Yemen	C0
French Guiana	DF	Korea (Rep. of)	61	Zambia	C3
Lebanon	64	Kuwait	62	Zimbabwe	C4

Table 5.2-22: Set Straps Data Fields

Field	Value (ASCII)
Data[0...1]	Strap ID: 07 – SCIP Timeouts 0B – Auto Lock 13 – Secure Voice Application Control 20 – Allow Speakerphone 23 – Allow Black Computer Port 25 – Allow Web Management Others – Reserved – do not use
Data[2...3]	SCIP Timeout Strap: 01 = Normal 02 = Extended 1 04 = Extended 2 07 = Extended 3 Example : AT~FH0702 selects Extended 1 SCIP timeouts
Data[2...5]	Auto Lock Strap: NOTE: Access control must be satisfied before changes are allowed. See also *Auto Lock* (page 61). Octets 2-3: 01 = Enabled 02 = Disabled Octets 4-5: 01 – 99 = the PIN timeout value in minutes. If the strap is set to Disabled, you must still provide Octets 4-5, but they are ignored by the phone. Example: AT~FH0B0115 enables Auto Lock and sets the timeout to 15 minutes.
Data[2...3]	Secure Voice Application Control Strap: NOTE: Access control must be satisfied before changes are allowed. See also *Application Control* (page 62). 01 – Enabled + AutoSecure ON 02 = Enabled + AutoSecure OFF 04 = Secure Voice Disabled (not recommended) Example: AT~FH1301 enables AutoSecure for voice.

Table 5.2-22: Set Straps Data Fields (continued)

Field	Value (ASCII)
Data[2...3]	Allow Speakerphone Strap: NOTE: Access control must be satisfied before changes are allowed. See also *Application Control* (page 62). 01 – Enabled 02 = Disabled Example: AT~FH2001 disables Speakerphone use.
Data[2...3]	Allow Black Computer Port: NOTE: This command has no effect during PSTN operation. Access control must be satisfied before changes are allowed. See also *Application Control* (page 62). 01 – Enabled 02 = Disabled Example: AT~FH2301 disables the Black Computer Port.
Data[2...3]	Allow Web Management: NOTE: This command has no effect during PSTN operation, but it will cause the phone to reboot. Access control must be satisfied before changes are allowed. See also *Application Control* (page 62). 01 – Enabled 02 = Disabled Example: AT~FH2501 disables Web Management.

Table 5.2-23: AT Command Error Codes

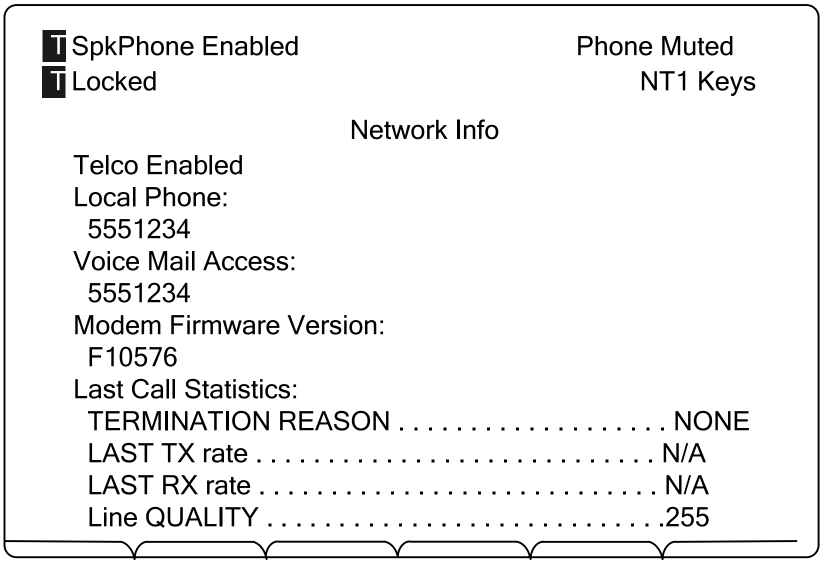
Error Code	Category	Description
0000	Processing Error	Failed to process the command due to an internal error.
0001	Message Not Supported	The message was not a recognizable AT Command.
0003	Invalid State	The AT Command is invalid in the current Terminal state.
0004	Invalid Data	Some or all data was out of range or the data string was of incorrect length.
0005	CRC or Signature Failure	The received data failed the associated CRC or Signature check.
0006	Master or User ID PIN Not Entered	The Master or User ID PIN needs to be entered before this command is acted on. Refer to *Access Control* on page 26 for additional information.
000B	Secure Call Setup Failure	The secure call could not be setup. Refer to *Table 4.3-1: Secure Call Error Messages* on page 39.
000C	Parameters Out of Order	Parameters which need to be entered in a specific order have been entered in the wrong order; e.g. ACL Header after DAO, or DAO after KMID.
000D	Overflow	An attempt has been made to enter too many parameters in a list with a limited number of parameters; e.g. more than 500 DAO and KMID parameters in the ACL list.

5.3 Phone Settings Menu

5.3.1 Network Information

Phone Settings >> Network Information

Select **Network Information** to display the network settings of the phone. *Figure 5.3-1* illustrates a sample Network Information display. Press **EXIT** when you are through viewing the data.



```
T SpkPhone Enabled                     Phone Muted
T Locked                                  NT1 Keys
                  Network Info
  Telco Enabled
  Local Phone:
   5551234
  Voice Mail Access:
   5551234
  Modem Firmware Version:
   F10576
  Last Call Statistics:
   TERMINATION REASON . . . . . . . . . . . . . . . . . . . NONE
   LAST TX rate . . . . . . . . . . . . . . . . . . . . . . . . . . . N/A
   LAST RX rate . . . . . . . . . . . . . . . . . . . . . . . . . . . N/A
   Line QUALITY . . . . . . . . . . . . . . . . . . . . . . . . . .255
```

Figure 5.3-1: Network Information Display

The first line under the **Network Info** header indicates that the phone is configured for PSTN operation. This is followed by the phone number and voice mail numbers configured for the phone and the firmware version number of the PSTN Connect accessory. The PSTN Connect accessory must be connected for its firmware version number to be displayed. The final section shows statistics associated with the last call.

5.3.2 Display Settings

Phone Settings >> Display Settings

The **Display Settings** dialog allows you to change the backlight intensity and display contrast.

5.3.2.1 Backlight

To change the Backlight intensity, scroll to **Backlight** and press **ENTER**. Use the up/down scroll keys to change the intensity, then press **ENTER** when you are satisfied.

5.3.2.2 Contrast

To change the contrast, scroll to **Contrast** and press **ENTER**. Use the up/down scroll keys to change the contrast, then press **ENTER** when you are satisfied.

5.3.3 Telco Settings

Phone Settings >> Telco Settings

Select **Telco Settings** to display the list of configurable settings for PSTN operation.

5.3.3.1 Country Code Select

Phone Settings >> Telco Settings >> Country Code Select

Select the Country Code Select menu to configure the PSTN Connect accessory for the telephony equipment in the country in which you are operating the vIPer Phone. The Country Code is used to match the electronic properties and telephony standards of the telephone service you are using. This may also be accomplished using the Select Country Code AT Command (AT+GCI) described in section *AT Command Support* (page 72).

WARNING: Check with your telephone service provider to verify which country code you should use before changing this setting. For example, you may find that the telephone service is using U.S. equipment even though you are not physically in the U.S. Use of an improper country code can cause the PSTN Connect accessory to function improperly or can cause more serious problems including damage to the PSTN Connect or telephone service equipment.

5.3.3.2 Network Quality

Phone Settings >> Telco Settings >> Network Quality

Select **Network Quality** to adjust the maximum data rate used for secure calls. The **Network Quality** menu allows you to select either **Normal** or **Low 4800**. The **Low 4800** setting can increase the secure call completion rate when placing calls over poor quality telephone networks.

WARNING: Setting **Network Quality** to **Low 4800** can cause interoperability problems with some devices including SGSM and some STEs. This setting should only be used if absolutely necessary.

NOTE: Setting the **Network Quality** *to* **Low 4800** *overrides the vIPer Phone's default modem speed (e.g. 9600). All secure voice calls will connect at 4800 bps max.*

5.3.3.3 2100Hz Detect

Phone Settings >> Telco Settings >> 2100Hz Detect

The 2100 Hz signal is used to initiate the beginning of the secure call setup process. Select the **2100Hz Detect** menu to adjust the length of time the signal must be present before the vIPer Phone will respond to it.

TIP: If false 2100 Hz detections occur due to background noise, set the **2100Hz Detect** to **Long** to increase the amount of time 2100 Hz must be present before secure call setup is initiated.

5.3.3.4 Local Phone Number

Phone Settings >> Telco Settings >> 2100Hz Detect

Select **Local Phone Number** to adjust the phone number shown on the top-level display. This value does not affect Caller ID information reported for your phone since that is configured on the telephone switch. Contact your telephone service department if you need to change your Caller ID information.

5.3.3.5 Voice Mail Number

Phone Settings >> Telco Settings >> Voice Mail Number

Select **Voice Mail Number** to specify the phone number to call to access your voice mail.

5.3.3.6 Precedence Dial Mode

Phone Settings >> Telco Settings >> Precedence Dial Mode

Select **Precedence Dial Mode** to select the dialing method for placing precedence calls (if supported by your telephone service). Select **Prefix Only** to use a numeric code to activate a precedence selection. Selecting **Menu and Prefix** allows prefix dialing but also displays precedence softkeys to simulate a 16-key dialpad. Contact your telephone service department to see if your telephone service supports the A, B, C, and D dialing digits before enabling the **Menu and Prefix** option.

5.3.4 Upgrade Network Processor Software

Phone Settings >> Upgrade Network Processor Software

Select **Upgrade Network Processor Software** to put the vIPer phone in the mode for updating the network software. After you confirm that this is what you intend, the vIPer Phone will reboot into the Code Upgrade mode. Consult the section on Code Upgrade and Recovery in the *Sectéra and TalkSECURE vIPer Phone Administrator's Manual* for instructions on how to update the software.

TIP: The vIPer Phone will only reboot once into Code Upgrade mode. If you need to return the phone to normal operation without upgrading the network software, reboot the phone by disconnecting and reconnecting the power supply.

6 Updating Network Software

Because the vIPer Phone must support many different networks it is necessary to provide the ability to separately update the network software. The Code Upgrade process is the means whereby the network software is updated. Normally your telecom service provider will ensure that you have the proper network software for your installation. Should you need to update the network software yourself, refer to *Upgrade Network Processor Software* (page 82).

7 Updating Security Software

The security software is separately updateable from the network software. You may obtain the software update package from your Security Administrator or by contacting *Customer Support* (page 95). Follow your organization's procedures for obtaining and loading software. Refer to the *Sectéra and TalkSECURE vIPer Software Update User's Manual*, included on the distribution CD packed with your vIPer Phone, for detailed instructions on updating your security software.

8 User Maintenance

The vIPer Phone requires the following minimal maintenance:

- Periodically cleaning the case with a soft, dry cloth,
- Checking the condition of the case, cables, and connections, and
- Periodically charging the internal battery if the phone is disconnected from a power source for long periods of time.

> WARNING: The vIPer Phone is equipped with an internal lithium ion rechargeable battery that provides power to critical circuitry. If this battery is allowed to discharge, your phone will lose its ability to place secure calls and will display “Tamper Detected.” The battery is sized to provide power to the circuitry for 48 months without recharging. If the phone is stored for long periods of time, it should be plugged into a power source for a minimum of two hours every 48 months to recharge the battery. If the phone is stored at extreme temperatures, either hot or cold, it should be recharged more frequently.

Store the phone in a cool, dry location (e.g. office environment) when not in use.

There are no user serviceable parts inside. Opening the case will render the phone cryptographically incapable. The case has tamper evident seals and is designed to facilitate inspection for tamper detection in environments where this is a concern.

> WARNING: Opening the case of the vIPer Phone will render it cryptographically incapable. Should a phone be opened it can still be used in the clear (assuming no circuitry is damaged in the process) but cannot place or receive secure calls. You must return the phone to General Dynamics for servicing. General Dynamics may refuse service if it sees evidence of tampering.

9 If You Have Problems

If you encounter problems using your phone, we suggest you first ensure that you have followed the instructions in this guide and any applicable supplements. Then work through the Troubleshooting Guide and finally call your telecom service provider for help. If these attempts fail to fix the problem, call *Customer Support* (page 95) for additional help.

9.1 Troubleshooting Guide

Table 9.1-1: Troubleshooting - General Problems

Problem	Fault	Solution
Display is blank	Lack of power	Verify that the provided power adapter is connected correctly and that the wall outlet has power. It is easy to reverse connections on the power adapter.
The display shows: **Error Detected Please Wait While Phone Resets**	Internal error	Write down the eight digit error code shown on the display, then disconnect the 10/100 LAN cable and reconnect it. If this fails to correct the problem, contact *Customer Support* (page 95).
The top level menu is never displayed.	Internal error	Disconnect the 10/100 LAN cable and reconnect it. If this fails to correct the problem, contact *Customer Support* (page 95).
The display indicates **Tamper Detected**	Loss of tamper variables	This display can result from a number of conditions: • The internal lithium battery has failed. • Someone pressed the Depot Return switch (see *Returns* on page 95). • Someone has attempted to open the case or otherwise tamper with the phone. Contact *Customer Support* (page 95) for repair.
The display indicates **Unauthorized or no device connected to BDI port. Attach PSTN Connect Module**.	PSTN Connect accessory not properly connected	Verify that you are using the Sectera PSTN Connect accessory and that it is securely connected to the BDI port, and then select the **Retry** softkey to reboot the phone. If this fails to correct the problem, contact *Customer Support* (page 95).

Table 9.1-2: Troubleshooting - Menu Access and Use

Problem	**Fault**	**Solution**
The PIN Menu option is not displayed	Access Control Configuration	Your vIPer Phone has not been configured with the Controlled or Restricted access control model. See *Access Control* (page 26) for more details.
You are unable to enter the Key Management Menu	Tamper detected	Your phone may have been tampered and must be returned for repair. Call *Customer Support* (page 95).
The Software Verification Result is **Software Verify Failed**	Security software compromised	Notify your security authority. DO NOT ATTEMPT TO PLACE A SECURE CALL. Contact *Customer Support* (page 95).
The Master PIN is not accepted and the Security Menu is not accessible	Deleted Master PIN	To recreate the Master PIN you first have to delete all existing Users. This will consequently delete all key material. You can then recreate the users and install new key material.

Table 9.1-3: Troubleshooting - Network Issues

Problem	Fault	Solution
Cannot access voice mail	Unable to reach voice mail server	This could indicate several possible problems: • Your phone is not configured with the correct phone number for the voice mail server. Contact your Telephone Service Provider. • Your voice mail server is down. Contact your Telephone Service Provider. • Your network does not provide voice mail service.
The phone never rings.	Network connectivity issues	Have someone call your phone to verify there is a problem. If it still does not ring, check the following: • Your telephone line may not be active or you may be connecting to the wrong telephone jack. Contact your Telephone Service Provider. • Your phone may be forwarding all your calls.
Voice quality is poor. Speech is choppy or missing segments. Calls may occasionally be dropped.	Network congestion	Contact your Telephone Service Provider. Note: The congestion may be on an external network and your local Telephone Service Provider may not be able to correct the problem.

Table 9.1-4: Troubleshooting - Software Update (Security Software)

Problem	Fault	Solution
Attempted to software update the phone and the PC Updater Application indicated that the phone could not be updated, or update "freezes".	Various	• Verify that the phone is receiving power. This may require connecting the power adapter if you are not receiving power from the Ethernet connection. Try removing and reapplying power. • Verify that the phone is properly connected to the host computer providing the update. • Use PC Updater 2.3 or later. If the problem persists, contact *Customer Support* (page 95).
The PC Updater application reports: ERROR: Invalid Product Code	Incorrect software update package	Obtain the correct software update package and try again.
The PC Updater application reports: ERROR: CommPortError	Host computer port configured incorrectly	Verify that PC Updater Baud rate is set for 57600. Remove and reapply power to the phone and try again.
The PC Updater application reports: ERROR: AT ERROR response received	Phone not entering software update.	Try the following: • Enter the Master PIN if the phone is in the Restricted mode or the UserID PIN if in the Controlled mode. • Verify that the phone's Configuration Menu Data Port Rate is set to 9600. PC Updater establishes communication with the phone at 9600 and then switches to the Baudrate displayed on its toolbar (e.g., 57600) to send the software packets. • If you are in Restricted mode and the Master PIN has been deleted, the phone will display **Master PIN Reqd No Master PIN**. You will need to delete all UserID PINs, which will consequently delete all key material. You can then perform Software Update. After the update, you will have to regenerate/reload all key material and recreate users. • If you are unable to enter the Key Management Menu, your phone may have been tampered. Contact *Customer Support* (page 95).

Table 9.1-4: Troubleshooting - Software Update (Security Software) continued

Problem	Fault	Solution
The software update stops at a high packet number (e.g. 44) with internal SCP error (0X51) and indicates "suse-response-timer-expired"	The computer is sending data too slowly.	Try the following: • Place the software update file (.spd) on your desktop • Restart PC Updater and reload the update file for each software update • Make sure you are using a standard serial cable – not a null modem cable. • Try a different COM port. Sometimes COM3 is used as a modem port – avoid this port. • Reboot your host computer. • Try a different (faster) host computer. If problems persist, contact *Customer Support* (page 95).
The PC Updater application reports: "ERROR: Timeout on AT command, resending," followed by "ERROR: Too many timeouts, stopping update"	PC Updater is not communicating with the phone	Try the following: • Verify the phone's Configuration Menu Data Port Rate is set to 9600. • Re-power the phone, restart PC Updater, and try again • If you are using a USB to serial adapter, try a plain serial cable instead. • Verify that you are using a plain serial cable, not a null modem cable. • Try a different COM port. Sometimes COM3 is used as a modem port – avoid this port. If the problem persists, contact *Customer Support* (page 95).
Software Update appeared to finish, but the phone never displays its top level menu.	Incomplete software update.	Repeat the software update process.

Table 9.1-5: Troubleshooting - Network Software Upgrade (Code Upgrade)

Problem	Fault	Solution
Phone displays **Terminal Unavailable – Code Upgrade Required – Contact System Admin**	Phone requires an update of the network processor software	The phone waits for a Code Upgrade file to be uploaded via its Web Interface and will not service any calls. Connect a PC to the LAN port using a cross-over cable and browse to the address of http://192.168.1.3 to start the Code Upgrade process. More detail is in the *Sectéra and TalkSECURE vIPer Phone Administrator's Manual*. See your COMSEC Custodian or telecom Security Administrator if you need help.

Table 9.1-6: Troubleshooting - Group Key Processing

Problem	Fault	Solution
Cannot go secure using a specific Group Key – **No Common Key** is displayed.	No matching group key	This scenario most often occurs when Group Key is entered manually into the phone. Use the Group Key Manager to load the keys if at all possible. If not, verify that the key was entered correctly in all phones that share the same group key. Finally, be sure that the phone you are trying to go secure with has the same group key as your phone and is really the phone you think it is. After all, the purpose of Group Key is to prevent going secure with unauthorized phones.
The phone has Group Keys and goes secure displaying **SECURE APK** or **PROTECTED** without <display ID> information.	No common Group Key and Non-mandatory Group Key use	Either: • One or more Group Keys has the Mandatory Exclusion Flag set to False, or • The Display ID field in the key is empty Note: Neither of these conditions is necessarily a problem. You should check with your Security Authority if you are unsure how your phone should behave in a given situation. If any Group Key has the Mandatory Flag set to FALSE the phone is not required to use any Group Key.
The phone has Group Key and cannot go secure with phones that do not have Group Key	All of the phone's Mandatory Exclusion Flags are set to TRUE	Verify with your Security Authority that you are allowed to go secure with phones that do not have Group Key. If allowed, load a Group Key that has a Mandatory Flag set to FALSE.

Table 9.1-7: Troubleshooting - Clear Call Processing

Problem	Fault	Solution
Unable to place a clear call	Phone has lost connectivity	Remove and reapply power to the phone. If this does not correct the problem, consult your telecom service provider.
Unable to reach off-network phones when dialing from the inbound call history	Off-network dialing	Often you are required to dial 9 (or some other digit) to seize an off-network line. From the inbound call history, select the number you wish to dial, press **View/Edit Dial**, scroll to the first digit, and press the special access code (usually 9). Go off-hook to initiate the call.

Table 9.1-8: Troubleshooting - Secure Call Processing

Problem	Fault	Solution
The APK Key was generated or UnivCert was enabled, but the phone indicates it is not keyed	APK was zeroized or UnivCert was disabled	Check the following: • Were all User IDs deleted? • Did someone activate the Depot Return switch (see *Returns* on page 95)? • Did someone zeroize the APK key? • Has the phone been compromised (e.g. case opened)? Regenerate the APK key or enable the UnivCert and try again. If the phone still indicates it is not keyed, contact *Customer Support* (page 95).
The phone will not go secure with another SCIP compatible phone	• You have incompatible Group Key, or • a phone is not keyed • Secure Voice Min/Max levels are incompatible • You may have network problems	• Verify that both phones have compatible Group Key, that both phones have at least one Group Key with the Mandatory Exclusion Flag set to FALSE, or that you are using Group Key. • Verify that both phones have generated an APK key or that both phones have enabled the UnivCert. • Verity that the Secure Voice Min/Max levels on both phones overlap each other. • On low quality networks, change the **Network Quality** to **Low 4800** and lower the **2100Hz Detect** threshold to **Short**. See *Network Quality* on page 81 and *2100Hz Detect* on page 81 for more information. • Try having the phone on the other end initiate secure.
The phone goes secure but prompts to revert to clear traffic in the middle of the call	• Your call may have been preempted • You may have received a call waiting signal	• Preemption signals from the telephone service will disrupt a secure call but will not be heard until you return to clear traffic. This is correct behavior on networks supporting MLPP. • Try dialing *70 to temporarily disable call waiting (or other code if required) before you dial a call on which you intend to go secure or contact your Telephone Service Provider to permanently disable call waiting on your line. Alternatively, you can also change **Network Quality** to **Low 4800** since lower data rates are not as sensitive to call waiting tones. See *Network Quality* on page 81 for more information.

9.2 Customer Support

Before contacting General Dynamics for warranty service for the vIPer Phone, follow all programming and operating steps as prescribed in this guide.

For technical questions or Maintenance/ Repair service information for the vIPer Phone, contact Customer Support:

Toll Free: (877) 230-0236
Commercial: (410) 850-4893
DSN: 644-1139
Fax: (410) 487-0252
Email: infosecsupport@gdc4s.com

9.3 Returns

Two recessed buttons are located under the base of your vIPer Phone. If you are a Sectéra vIPer Phone user, consult the *Sectéra vIPer Phone Supplement* on the use of these buttons. If you are a *Talk*SECURE vIPer user, do not depress either of these buttons unless instructed to do so by *Customer Support*.

- The Depot Return switch (DEPOT RTN) removes certain data from the phone that may make it difficult to troubleshoot and renders it cryptographically incapable.
- The Factory Use Only switch (FCTY USE ONLY) holds certain processors in reset. Aside from making the phone temporarily non-operational it has no lasting effect. It should not be actuated by a user.

The General Dynamics *Customer Support* will provide detailed shipping and handling instructions, including assigning the Return Authorization Number to any user whose phone that requires service.

When you contact *Customer Support* for shipping authorization, you will be given complete instructions regarding packaging and other safeguards. Plan on the following minimal guidelines for returning the vIPer Phone:

- Include a description of the fault
- Provide a return shipping address, contact name and phone number
- Zeroize all key material and delete all users

If possible, ship the vIPer Phone in its original shipping container.

9.4 Warranty Terms and Conditions

Sectéra vIPer Phone users should consult the *Sectéra vIPer Phone Supplement* for applicable warranty provisions.

The vIPer Phone contains no user serviceable components. Any attempt to open the vIPer Phone voids the warranty.

Seller warrants that all of its products sold hereunder will at the time of delivery be free from defects in materials and workmanship and will conform to Seller's applicable specifications or, if appropriate, to specifications accepted by Seller. Therefore, Seller's obligation hereunder shall be limited to, at Seller's option, either correcting, refunding the purchase price of or replacing any product for which written notice of nonconformance hereunder is received by Seller within the two-year warranty time from the date of delivery, provided that such nonconforming product is, with Seller's prior authorization, returned to Seller's plant within 30 days after such written authorization at Buyer's expense. Additional warranties may be purchased.

IN NO EVENT WILL SELLER BE LIABLE FOR ANY INCIDENTAL OR CONSEQUENTIAL DAMAGES.

This warranty shall not apply to any products in other than their original condition, or to any products which Seller determines have, by Buyer or otherwise, been subjected to operating and/or environmental conditions in excess of the maximum values in the applicable specifications or operating instructions, or otherwise have been the subject of misuse, neglect, improper installation, repair, alteration or damage.

THIS WARRANTY EXTENDS TO BUYER ONLY AND NOT TO BUYER'S CUSTOMERS OR USERS OF BUYER'S PRODUCTS AND IS IN LIEU OF ALL OTHER WARRANTIES WHETHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR PARTICULAR PURPOSE.

Servicing of the vIPer Phone is limited to specific trained personnel.

NO USER SERVICABLE PARTS INSIDE

9.5 Disposal

Users of the Sectéra vIPer Phone should consult the *Sectéra vIPer Phone Supplement* for disposal instructions.

The vIPer Phone contains materials that are not compliant with European standards for electronic products. These materials include lead-based solder and a lithium ion battery. Consult with local authorities before disposing of the phone.

The phone should be disposed of in accordance with local regulations.

10 General Information

10.1 Applicable Standards

The vIPer Phone implements the following standards and protocols including:

10.1.1 Government Standards

SCIP-210	Secure Communications Interoperability Protocol Signaling Plan
SCIP-231	Secure Communications Interoperability Protocol ECMQV/AES Cryptography Specification.
MELP	Multiple Excitation Linear Prediction Vocoder specification
AES	Advanced Encryption Standard
SHA-1	Secure Hash Algorithm-1

10.1.2 International Telephone Union (ITU) Standards

V.32	Modem Operating at Data Rates Up to 9600 bps
V.34	Modem Operating at Data Rates Up to 33600 bps
G.729	Vocoder specification (annex A and D)
G.711	Vocoder specification
G.723.1	Vocoder specification
G.726	Vocoder specification

10.1.3 EIA/TIA Standards

RS232F	Serial port specification

10.1.4 Other Standards

USB	Universal Serial Bus Specification (v1.1)

10.2 Sectéra Product and Sales Information

For other general product and sales information, you may contact Sectéra Product and Sales Information:

Toll Free: 888-897-3148
Commercial: 781-455-2800
Fax: 781-455-5555
Email: infosec@gdc4s.com

Visit the Sectéra Website at:
www.gdc4s.com/sectera

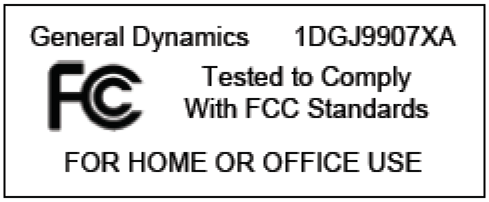
10.3 Approvals and Compliance

10.3.1 EMI/EMC

The vIPer Phone and PSTN Connect comply with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and
(2) This device must accept any interference received, including interference that may cause undesired operation.

WARNING: Changes or modifications to the item not expressly approved by General Dynamics could void your authority to operate the equipment.



General Dynamics 1DGJ9907XA

FC Tested to Comply With FCC Standards

FOR HOME OR OFFICE USE

The PSTN Connect also complies with EN55022 and EN50082-1. This class B digital apparatus applies to Canadian ICES-0003.

10.3.2 Safety Approvals

The vIPer Phone and PSTN Connect have been tested and found to comply with IEC 60950, 3rd Edition, UL Std 1950, 3rd Edition, CAN/CSA Std C22.2 950, 3rd Edition, ACA, TS001-1997, Safety Requirements for Customer Equipment, and AS/NZS 3260-1993, Safety of Information Technology Equipment Including Electrical Business Equipment, including Amendments A1, A2, A3 and A4.

10.4 Applicable Patents

Manufactured under one or more of the following U.S. patents:

6,219,420

5,341,427

D434,408

5,995,628

Other patents are pending.

Universite de Sherbrooké, France, Télécom Nippon Telegraph and Telephone Corporation own or may own or have licenses to patents or copyrights necessary to comply with the G.729 Standard contained in the equipment or software named herein.

General Dynamics reserves the right to make changes to its products and specifications at any time and without notice.

10.5 Specifications

vIPer Phone	*PSTN Connect*
Size Width 10 in. Depth 3 in. (without footstand) Length 9.5 in. Weight 4.5 lbs (with footstand) Volume 285 cu in.	***Size*** Width 1.4 in. Depth 1.0 in. Length 2.4 in. Weight 0.05 lbs Volume 3.4 cu in.
Red Interfaces RS-232 data port DS-101 Key Fill Headset port USB port	
Black Interfaces 10/100BaseT to LAN/WAN 10/100BaseT to Black Computer USB port	***Interfaces*** USB 2.0 port RJ-11 FXO port
Power Powered over Ethernet (802.3af) -or- AC power 110 to 220 VAC, 50-60 Hz 8 Watts maximum operating	***Power*** DC power 5V @ 0.5A (via USB)
Speech Processing Non-secure: G.711, G.729A Secure: G.729D, MELP	***Speech Processing*** Non-secure: G.711
Environment	***Environment***
MIL-STD-810F (temperature, humidity, vibration, shock and altitude)	MIL-STD-810F (temperature, humidity, vibration, shock and altitude)
Operational 0ºC to +50ºC (32ºF to 122ºF)	Operational 0ºC to +50ºC (32ºF to 122ºF)
Storage –30ºC to +80ºC (–22ºF to +176ºF)	Storage –30ºC to +80ºC (–22ºF to +176ºF)
Humidity 95% (non-condensing)	Humidity 95% (non-condensing)
Altitude Sea level up to 40,000 ft (non-operating)	Altitude Sea level up to 40,000 ft (non-operating)
Sea level up to 10,000 ft (operating)	Sea level up to 10,000 ft (operating)
Approvals	***Approvals***
TSG: CNSSI-5000/5001	TSG: TSG-5

vIPer Phone	***PSTN Connect***
Safety: UL 60950, EN60950, IEC60950	Safety: UL 60950, EN60950, IEC60950
EMI/EMC: FCC Part 15 subpart B, Class B	EMI/EMC: FCC Part 15 subpart B, Class B EN55022/EN55024, AS/NZS 3548
TEMPEST	Telco: TIA/EIA/IS 968-A-5, TBR-21, IC CS-03 Issue 8, Part 1, AS/ACIF S002:2001, PTC 200: Iss2, Oct 1997, Amend. 1 1998

Index

GENERAL DYNAMICS

8220 East Roosevelt Street

Scottsdale, AZ 85257

Sectéra Product and Sales Information
(888) 897-3148 or (781) 455-2800

Maintenance/Repair
(877) 230-0236 or (410) 850-4893

www.gdc4s.com/sectera

68-P49741G Rev A