

# **GENERAL DYNAMICS**

## C4 Systems



### ***Wireless and Wireline***

### **Products**

### **Frequently Asked Questions**



Frequently Asked Questions

Table of Contents

- 1. Why do I need secure products and solutions?..... 4**
  - 1.1 Why do I need secure telecommunications?..... 4
  - 1.2 My phone conversations have never been wiretapped or listened to, so why should I think that they might be in the future? ..... 4
  - 1.3 How easy is it for someone to eavesdrop on a digital wireless phone conversation that is not secure and how much does it cost? ..... 4
  - 1.4 How easy is it for someone to wiretap a telephone conversation that is not secure?..... 5
- 2. What secure communication products are available from General Dynamics C4 Systems and what makes them secure? ..... 5**
  - 2.1 Which Sectéra products are available for secure voice? Which Sectéra products are available for secure data? ..... 5
  - 2.2 What is encryption? ..... 7
  - 2.3 How will my conversations be protected from eavesdropping or wiretapping if I'm using the Sectéra Wireless or Wireline products? ..... 8
  - 2.4 How do the Sectéra Wireless phones compare to competing products?..... 8
- 3. What is GSM technology and how universal is GSM coverage? ..... 8**
  - 3.1 What is GSM?..... 8
  - 3.2 Why is GSM technology used for Sectéra Wireless phones? ..... 9
  - 3.3 What's the significance of using a Tri-band GSM phone? ..... 9
  - 3.4 What type of GSM service coverage is available in the U.S. and abroad? ..... 9
  - 3.5 Doesn't GSM already have encryption built in?..... 10
- 4. What other products will Sectéra Wireless and Wireline products communicate with? ..... 10**
  - 4.1 If I am using a Type 1 Sectéra Secure Wireless Phone, what device is required on the other end for the call to be secure? ..... 10
  - 4.2 What is SCIP signaling, and why is it important? ..... 11
  - 4.3 What steps are required for a Type 1 Sectéra Secure Wireless Phone to communicate securely with a TalkSECURE™ Wireless phone?..... 11
  - 4.4 Do Sectéra products communicate with the STU-III? ..... 11
  - 4.5 Does the TalkSECURE key management system allow you to restrict secure communications to a defined group of users? ..... 11
  - 4.6 How does Group Key work?..... 12
- 5. How do I get started with Sectéra products? ..... 12**
  - 5.1. How do I order Sectéra Wireless and Wireline products?..... 12
  - 5.2. What other items do I need to get started? ..... 12
  - 5.3. When subscribing to wireless service, what does my GSM Service Provider need to know for Sectéra Wireless phones?..... 13
  - 5.4. How will my monthly service fees be affected?..... 14
- 6. What are some other common questions about the operation of Sectéra Wireless phones?..... 14**
  - 6.1 Why do I need to have two phone numbers for Sectéra Wireless phones? ..... 14
  - 6.2 What are some typical usage scenarios for Sectéra Wireless phones? ..... 14
  - 6.3 Can Sectéra Wireless phones be used as a regular cell phone (without encryption)? What do I need to do to place it in this mode?..... 15
  - 6.4 If I'm in the middle of a non-secure call and decide the call should be secure, how easy is it to change to secure mode? ..... 15
  - 6.5 How good is the voice quality of a secure call? What about delay time?..... 15

# Sectéra® Wireless and Wireline Products

## Frequently Asked Questions

6.6	How long does it take to get a secure call connected? .....	15
6.7	I am based in the U.S. — what do I need to do before I travel abroad? .....	15
6.8	How is my Secure Module PIN assigned? .....	16
6.9	How do I upgrade my phone as new functionality becomes available? .....	16
6.10	What should I do if I am not successful in making a secure call? .....	16
6.11	What if the “Secure Voice” option is not displayed on the Dialing or Phonebook Menu option when I try to make a secure call? .....	17
<b>7.</b>	<b>What security procedures do I need to use with Sectéra Wireless phones? .</b>	<b>17</b>
7.1	What do I do if my Sectéra Wireless phone is lost or stolen? .....	17
7.2	If my Sectéra Wireless phone is lost or stolen, will someone else be able to use it to make a secure call? .....	17
7.3	What other security procedures do I need to be aware of to use these products? .....	18
<b>8.</b>	<b>What are some other common questions about the operation of Sectéra Wireline Terminals? .....</b>	<b>18</b>
8.1.	Does each user need a Sectéra Wireline Terminal assigned to them? .....	18
8.2.	My office telephone system is digital, not analog. Will I be able to use Sectéra Wireline Terminals at the office as well as at home? .....	18
	<b>Glossary .....</b>	<b>19</b>

## Frequently Asked Questions

### 1. Why do I need secure products and solutions?

#### 1.1 Why do I need secure telecommunications?

Not everyone has a need for secure exchange of voice or data; however, some professions have a responsibility to manage and control classified, sensitive, and/or private communications on a daily basis. For example, people who are responsible for financial information, public safety, strategic information and/or trade secrets. If your organization's information or communications fell into the wrong hands, would it be harmful to you, your organization or your country? If so, you need secure telecommunications.

Additionally, the Department of Defense issued a Memorandum dated September 25, 2002, and titled "Pentagon Area Common Information Technology Wireless Security Policy" that requires "encryption via NIST FIPS-approved or NSA-approved encryption mechanisms while in the wireless environment."

#### 1.2 My phone conversations have never been wiretapped or listened to, so why should I think that they might be in the future?

Unfortunately, they may have been and you would not even know about it. Unlike the theft of a physical asset, there may be no evidence. As with all types of security, **prevention** is the key. Your organization probably already employs the following types of security to prevent theft of physical assets and data, or to protect employees, assets and data from harm (even if they have never been compromised in the past):

- Intrusion Detection and Control
- Access Management Systems, such as card readers and photo ID badges
- Video Surveillance
- Anti-Virus Protection for Computers
- Firewall Protection for Computers attached to the Internet

#### 1.3 How easy is it for someone to eavesdrop on a digital wireless phone conversation that is not secure and how much does it cost?

Eavesdropping, and security in general, is not a black-and-white process. It's never a case of "this system can be compromised but that one cannot." Instead, it is a matter of how much time it will take and how much

## Frequently Asked Questions

it will cost to break into a particular system. The first generation of analog cellular phones were very simple to listen to – for something on the order of a few hundred dollars, scanners could be purchased on the open market that would let a third party listen to a wireless phone conversation. With the second generation of digital wireless phones the problem became much more difficult for the casual listener, but still very much within the scope of professional eavesdroppers. Authorized and unauthorized test equipment that allows a third party to listen to private digital wireless phone conversations can be purchased for a few thousand dollars. In general, physical access is not required for eavesdropping on wireless phone conversations. The only requirement for an eavesdropper in the same approximate location as the intended target is to obtain test equipment that will allow him to receive and decode the RF (radio frequency) transmissions from the target phone. If the wireless phone call terminates with a party connected to the Public Switched Telephone Network ([PSTN](#)), the opportunity exists to wiretap that conversation from the wireline side.

### **1.4 How easy is it for someone to wiretap a telephone conversation that is not secure?**

For a standard landline telephone, the problem of wiretapping becomes one of physical access. Somewhere between the two ends of the conversation, the eavesdropper needs to obtain physical or electrical access to the transmission channel. This could be at the premises of one party or the other, it could be at a local Private Branch Exchange ([PBX](#)), it could be at a Central Office ([CO](#)), or it could be at a long-haul carrier facility between COs. The cost of the required equipment varies depending on the access point, but in general is minimal. If an eavesdropper has access to the local loop at one location, for example, the equipment could be as simple as a \$19.95 tape recorder. If the only access point is a microwave link between two COs, additional equipment to receive and decode the conversation would be required.

## **2. What secure communication products are available from General Dynamics C4 Systems and what makes them secure?**

### **2.1 Which Sectéra products are available for secure voice? Which Sectéra products are available for secure data?**

The Sectéra Architecture is employed by a family of products and offers high assurance security solutions that are totally software programmable,

## Sectéra® Wireless and Wireline Products

### Frequently Asked Questions

algorithm agile, compatible with interoperability standards and are application, network and media independent.

The Sectéra Secure Wireless Phone for GSM is available for high assurance secure voice and data communications using [Type 1](#) encryption for authorized U.S. Government personnel. The National Security Agency (NSA) has certified the secure phone's ability to protect information classified Top Secret and below. The phone also includes the Advanced Encryption Standard ([AES](#)) to provide interoperability with the [TalkSECURE™](#) Wireless and Wireline products. The Sectéra Secure Wireless Phone consists of the General Dynamics clip-in Secure Module and the Motorola Timeport™ tri-band phone, which has the features and convenience expected in a commercial wireless product.

The Sectéra Wireline Terminal is certified by the NSA to protect information classified Top Secret and below, using Type 1 encryption algorithms for secure voice and data communications. The Wireline Terminal also includes AES for interoperability with TalkSECURE Wireless and Wireline products. The Sectéra Wireline Terminal is a compact, lightweight device that connects to a standard analog phone, a fax machine or personal computer. The Wireline Terminal can be adapted to secure communications over ISDN networks. The Wireline Terminal with the Black Digital Interface (BDI) can be used to protect communications over a variety of satellite applications, including Iridium®, Inmarsat®, Globalstar and Thuraya satellite networks. Additionally, the terminal can be used to secure voice and data for mobile networks, other Hayes AT-compatible communication devices and can provide secure data rates up to 128 Kb/s over a landline digital network when connected to an ISDN adapter.

The Sectéra vIPer™ Phone provides the latest technology for secure, end-to-end Voice over IP and PSTN\* networks. Using SCIP signaling and commercial open standards, the vIPer Phone is certified to protect information classified Top Secret and below including Sensitive But Unclassified (SBU), and is available to support multiple key-sets for U.S. government sponsored interoperability (e.g., NATO and coalition). Built to provide seamless communications with legacy phones and encryption systems, the secure vIPer phone is software programmable with extensive memory to easily accommodate future upgrades and functionality.

*\* PSTN availability expected 3Q 2008 as an option*

The Sectéra Edge™ smartphone converges secure wireless voice and data by combining the functionality of a wireless phone and PDA — all in one easy-to-use handheld device. Developed for the National Security

## Sectéra® Wireless and Wireline Products

### Frequently Asked Questions

Agency's Secure Mobile Environment Portable Electronic Device (SME PED) program, the Sectéra Edge is certified to protect wireless voice communications classified Top Secret and below as well as access e-mail and websites classified Secret and below via high-speed GSM or CDMA cellular networks worldwide. The Sectéra Edge is the only SME PED that switches between an integrated classified and unclassified PDA with a single key press.

TalkSECURE products use the Sectéra Architecture and are designed for federal, state, local and international government officials, public safety officers, emergency response personnel and business users. Export controls for TalkSECURE products fall under the jurisdiction of the U.S. Department of Commerce.

The TalkSECURE Wireless phone is available for high assurance secure voice and data communications using the Advanced Encryption Standard (AES) to protect Sensitive But Unclassified (SBU) information. The TalkSECURE Wireless phone consists of the General Dynamics clip-in Secure Module and the Motorola Timeport™ tri-band phone, which has the features and convenience expected in a commercial wireless product.

The TalkSECURE Wireline terminal is available for high assurance secure voice and data communications, using AES to protect SBU Information. The TalkSECURE Wireline connects to a standard analog phone, fax machine or personal computer.

TalkSECURE Digital connected to a portable satellite phone is available for high assurance secure communications using AES.

The TalkSECURE vIPer phone provides the latest technology for secure, end-to-end Voice over IP and PSTN\* networks, using AES (Advanced Encryption Standard) encryption to protect SBU (Sensitive But Unclassified) communications. Built to provide seamless communications with legacy phones and encryption systems, the secure vIPer phone is software programmable with extensive memory to easily accommodate future upgrades and functionality.

*\* PSTN availability expected 3Q 2008 as an option*

#### **2.2 What is encryption?**

Encryption protects voice and data by encoding it at the transmitting point and decoding it at the receiving point. This means that plain text is converted into an unintelligible form and then converted back to plain text. The coding scheme used is called an algorithm. Sectéra certified [Type 1](#)

## Frequently Asked Questions

encryption products use U.S. Government National Security Agency (NSA) endorsed cryptography systems. The algorithms used in Sectéra products use cryptographic keys that are changed at the beginning of every call to ensure the coding schemes are unique to each session. [TalkSECURE](#) products use the [AES](#) algorithm, which is the current commercial encryption standard available from NIST (National Institute of Standards and Technology).

### 2.3 How will my conversations be protected from eavesdropping or wiretapping if I'm using the Sectéra Wireless or Wireline products?

The Sectéra Wireless and Wireline products perform “end-to-end” encryption; that is, they encrypt the conversation at one end and do not decrypt it until it arrives at the other end. Even if access is obtained by an eavesdropper at some intermediate point (such as at the [local loop](#); a Public Branch Exchange ([PBX](#)); a Central Office ([CO](#)); a long-haul carrier between COs; or, in the case of a wireless call, the transmitted Radio Frequency signal) the signal obtained would be encrypted and, therefore, unusable by the eavesdropper. **Note:** this end-to-end aspect means that compatible equipment must exist at both ends of the conversation.

### 2.4 How do the Sectéra Wireless phones compare to competing products?

The Sectéra Wireless phones are the only wireless secure solutions available today offering all of these benefits:

- *High assurance [Type 1](#) and/or [AES](#) end-to-end security.*
- *[SCIP](#) (Secure Communication Interoperability Protocol) compliance*
- *Secure interoperability between Type 1 and AES secure products*
- *Secure interoperability between wireless and wireline products*
- *High-quality voice without significant delays*
- *Access to commercial GSM wireless networks available worldwide*
- *Competitively priced*
- *Easy to use.*
- *Proven with more than 34,000 units deployed worldwide*

## 3. What is GSM technology and how universal is GSM coverage?

### 3.1 What is GSM?

[GSM](#) stands for Global System for Mobile Communications. GSM is an extremely successful wireless technology. GSM has superior coverage

## Frequently Asked Questions

with over 200 countries and accounts for 85% of the world's digital mobile market. With over two billion wireless subscribers, GSM is the fastest growing wireless communications technology in the U.S. and worldwide. (See [www.gsmworld.com](http://www.gsmworld.com) for more information.)

### 3.2 Why is GSM technology used for Sectéra Wireless phones?

GSM began primarily as a European standard with very little application in the Americas and Asia. Its popularity increased in Europe exponentially during the 1990s as wireless service providers in other areas began to become aware that GSM infrastructure equipment was becoming less expensive than other technologies to buy, operate, and maintain due to the economies of scale. As a result, GSM systems began to appear in North America, South America, and Asia during the late 1990s. It is the most popular digital wireless standard worldwide today, and as a result equipment vendors offer the most choices for supporting equipment. Phone manufacturers offer GSM-compatible phones with all the latest features. The total number of GSM users continues to increase at considerably higher rates than other technologies. There is another very important reason for choosing this technology for our product. The GSM infrastructure supports data calls using “transparent” services, allowing the transmission of encrypted messages to occur without significant delays. GSM is the only widespread digital wireless technology today that has implemented a transparent data mode for use by subscribers.

### 3.3 What’s the significance of using a Tri-band GSM phone?

Motorola’s TimePort phone provides Tri-band coverage, which means that the phone can be used in any part of the world with GSM coverage, using the 900/1800/1900 MHz frequency spectrum.

### 3.4 What type of GSM service coverage is available in the U.S. and abroad?

GSM accounts for approximately 85% of the global digital wireless market today with over 400 Service Providers. GSM is the fastest growing network in North America. Coverage in North America extends from Mexico to Canada and every state in the U.S. International roaming lies at the cornerstone of GSM’s success. GSM alliances make it possible to roam from the U.S. to countries in all continents except Antarctica. GSM Service Providers make up-to-date coverage maps available at [www.gsmworld.com/roaming/gsminfo](http://www.gsmworld.com/roaming/gsminfo) where you can select the country

## Frequently Asked Questions

and GSM network operator to find specific service coverage and roaming agreements.

### 3.5 Doesn't GSM already have encryption built in?

The [GSM](#) specifications include an over-the-air encryption. Although this is better than no encryption at all, there are some limitations involved. First, this encryption takes place only on the airlink portion of the communication channel. It is encrypted at the phone and decrypted at the base station, leaving the rest of the channel (interface to the Public Switched Telephone Network [[PSTN](#)], long-haul carrier, Central Office [[CO](#)], Private Branch Exchange [[PBX](#)], [local loop](#), etc.) vulnerable to eavesdropping or wiretapping. Second, the user does not control whether or how this encryption is used. The wireless Service Provider decides whether the encryption will be enabled on any given call. In some cases, local governments determine whether the GSM airlink encryption can be used. All of this results in users having little control over the security of their calls. Third, the encryption employed within the GSM specifications is at a much lower level of assurance (not as secure) than that provided by the Sectéra [Type 1](#) and [TalkSECURE](#) products.

## 4. What other products will Sectéra Wireless and Wireline products communicate with?

### 4.1 If I am using a Type 1 Sectéra Secure Wireless Phone, what device is required on the other end for the call to be secure?

The Sectéra Secure Wireless Phone will communicate in [Type 1](#) secure mode with:

- Type 1 Sectéra Secure Wireless Phones
- Type 1 Sectéra Wireline Terminals connected to a desktop phone
- Type 1 Sectéra BDI Terminal connected to a satellite phone
- Secure Terminal Equipment ([STE](#)) terminal (fitted with the [SCIP](#) 2.2 upgrade kit and the SCIP 2.0 hardware upgrade)
- SCIP-compatible devices

The Type 1 Sectéra Secure Wireless Phone will communicate in [AES](#) secure mode with a [TalkSECURE](#) Wireless phone or with a TalkSECURE Wireline terminal connected to a desktop phone.

## Frequently Asked Questions

### 4.2 What is SCIP signaling, and why is it important?

[SCIP](#) (Secure Communication Interoperability Protocol) is a signaling scheme that defines all the necessary information to allow various vendors to build interoperable cryptographic equipment utilizing U.S. Government [Type 1](#) encryption. Different vendors can build SCIP-compatible communication devices that allow their respective users to conduct a Type 1 encrypted conversation or exchange Type 1 encrypted data between them. SCIP signaling is also used to establish secure communications between vendor proprietary devices such as the [TalkSECURE](#) Wireless and Wireline products.

### 4.3 What steps are required for a Type 1 Sectéra Secure Wireless Phone to communicate securely with a TalkSECURE™ Wireless phone?

The [Type 1](#) user needs to generate the encryption key, or Automatic Public Key ([APK](#)), if this has not already been completed. This can be accomplished through the “Encryption Management” menu. When a secure call is placed to or received by a [TalkSECURE](#) Wireless phone, the Type 1 user will be prompted that a “Secure Downgrade” is taking place and they must respond “Yes” to continue.

### 4.4 Do Sectéra products communicate with the STU-III?

The [STU-III](#) will not directly communicate with the Sectéra products in the secure mode. STU-III is an analog-based signaling plan that uses legacy technology and is not compatible with the current [SCIP](#) (digital) signaling plan. The Sectéra Wireline Terminal can interoperate to STU-III phones when in “bypass” mode and with other SCIP devices when in “FNBDT” mode.

The Sectéra GSM Phone, Wireline Terminal and vIPer phone are cost-effective STU-III replacements. The GSM phone and Wireline Terminal are compact and easily transportable making an ideal secure solution not only for the desktop, but also on-the-move. The Sectéra vIPer Phone offers more features and eliminates the need for multiple desktop phones as it is used for regular calls, Type 1 and non-Type 1 voice and data.

### 4.5 Does the TalkSECURE key management system allow you to restrict secure communications to a defined group of users?

The TalkSECURE Group Key feature allows organizations to generate and load their own keys in TalkSECURE devices in order to restrict secure communications to defined groups of users. TalkSECURE Wireless and

## **Frequently Asked Questions**

Wireline products implement General Dynamics' Automatic Public Key (APK) management system. APK allows all TalkSECURE users to communicate with all other TalkSECURE users, even if they are from different countries or organizations. This ubiquitous interoperability and "out of the box" key management provided by APK is a significant benefit for most users. However there are situations when organizations prefer to limit secure communications to a closed group or groups.

### **4.6 How does Group Key work?**

The organization designates a Systems Administrator (SA). The SA generates and loads up to 10 different Group Keys. To load the Group Key into a TalkSECURE device, the SA may use the PC-based Group Key Tool, provided by General Dynamics at no cost. If there is more than one Group Key, the SA designates the Priority of each Group Key, so that the most preferred common key is utilized for secure calls between two users. The SA also selects whether the Group Key is Mandatory or Optional. If all of the Group Keys in a device are Mandatory, secure communications are limited to group members; that is, users cannot interoperate securely with other TalkSECURE users using APK. If any Group Key in the device is Optional, the users may interoperate securely with other TalkSECURE users using APK, but the Group Keys are given higher preference than APK. If the Group Key is used during a secure call, the device will show the Display ID information of the Group Key being used. In order to make secure calls with devices loaded with Group Keys, APK needs to be generated in the device by the user or SA.

## **5. How do I get started with Sectéra products?**

### **5.1. How do I order Sectéra Wireless and Wireline products?**

For information on ordering any of the Sectéra Wireless or Wireline products and accessories, call General Dynamics at 1-781-455-2800 or toll-free at 888-TYPE-1-4-U (888-897-3148).

### **5.2. What other items do I need to get started?**

1. For the Sectéra Wireless phones, subscribe to [GSM](#) service and order a [SIM](#) card from the GSM Service Provider. The service is separate from the phone and your Service Provider will need to activate the phone before you can use it. Service Providers should be selected based on their rate plans, as well as the user's requirements for local,

## Frequently Asked Questions

national and international coverage and roaming (see [3.4](#) for information on GSM Service Provider coverage and [www.gdc4s.com/sectera/service](http://www.gdc4s.com/sectera/service) for GSM Service Provider contact information). The Service Provider must offer Circuit Switched Data Services (see [5.3](#)).

2. For the Sectéra Wireline Terminals (or TalkSECURE Wireline terminal, or Sectéra BDI Terminal or TalkSECURE Digital), if they will be used with a digital telephone system, users should have their telecommunications department run a separate analog phone line, or use an analog adapter supported by their digital telephone system (see [8.2](#)).
3. For Sectéra BDI Terminal or TalkSECURE Digital, subscribe to satellite service from the Service Provider.
4. When Sectéra Type 1 and TalkSECURE products are initially shipped, they will not contain encryption key information. [Type I](#) users must arrange with their COMSEC Custodians for the ordering from the Electronic Key Management System ([EKMS](#)) and loading of the encryption keys. The Type 1 key can be loaded from a Data Transfer Device (DTD). A key fill cable accessory should be ordered with the phone in order to complete this step. [TalkSECURE](#) users (and Type 1 users that require secure communications with TalkSECURE users) need to generate the Automatic Public Key ([APK](#)). This can be accomplished through the “Encryption Management” menu.

### **5.3. When subscribing to wireless service, what does my GSM Service Provider need to know for Sectéra Wireless phones?**

Typically, when a user subscribes to a wireless service the Service Provider also provides a wireless phone, which is set up according to the service options ordered by the new subscriber. [GSM](#) is somewhat unique in that each GSM phone contains a Subscriber Identity Module ([SIM](#)) card containing information about the services ordered by the user. This SIM card can be moved from phone to phone and essentially becomes the identity of the phone. The subscriber’s phone number, for instance, is associated with the SIM card rather than with the phone. For Sectéra products, users will obtain the secure phones through General Dynamics C4 Systems and the wireless service through a local Service Provider (see [www.gdc4s.com/sectera/service](http://www.gdc4s.com/sectera/service) for contact information). A new subscriber will also need to obtain the SIM card from the Service Provider, set up with the following:

- Regular *Voice* Service
- 9600 BPS Asynchronous v.32 Transparent Circuit Switched *Data* Service with Mobile Originate (MO) and Mobile Terminate (MT) —

## Frequently Asked Questions

the user must specify that this is provided on a separate phone number from the voice number

- International Roaming (if you plan to use GSM and/or secure voice outside of the U.S.)

### 5.4. How will my monthly service fees be affected?

Monthly service fees are determined by your [GSM](#) or Iridium Service Provider's rate plans. Typically you will be charged for usage on the voice service as well as the data service. Other possible fees you may incur from your GSM Service Provider include domestic roaming, international roaming, long distance and/or charges for other features offered by your Service Provider.

## 6. What are some other common questions about the operation of Sectéra Wireless phones?

### 6.1 Why do I need to have two phone numbers for Sectéra Wireless phones?

Regular (non-secure) phone calls are made using your [GSM](#) Service Provider's *voice* service. Secure calls are made using your GSM Service Provider's *data* service, so that they may be encrypted. Setting up your secure service as a data service ensures that all of the system components and protocols (such as modems, if required) will be available for a secure voice or data call. Most GSM systems do not support a mode change from voice to data during the same call.

### 6.2 What are some typical usage scenarios for Sectéra Wireless phones?

There are two common usage scenarios. First is a secure call between two Sectéra Wireless phones. In this case, the call initiator may wish to place a call using the regular *voice* (non-secure) phone number and indicate that they will call back in secure mode. This ensures both parties have enabled secure mode by entering their Secure Module Personal Identification Number ([PIN](#)). Whether they have prearranged the secure call or not, the call initiator places the secure call by entering the secure (*data*) phone number, selecting "Secure Voice" from the user menu and pressing the SEND key.

In the second scenario, a secure call is made between a Sectéra Wireless phone and a Sectéra Wireline Terminal connected to a desktop phone. In

## Frequently Asked Questions

this situation, the wireless user establishes the secure voice call as in the previous paragraph, using the telephone number of the desktop phone connected to the Sectéra Wireline Terminal.

### **6.3 Can Sectéra Wireless phones be used as a regular cell phone (without encryption)? What do I need to do to place it in this mode?**

Yes, you can use Sectéra Wireless phones in regular (non-secure) mode by following the standard steps as described in the Motorola Timeport User's Manual, and you would *not* select "Secure Voice" from the user menu. To receive a regular (non-secure) call, you would give callers your *voice* (non-secure) phone number.

### **6.4 If I'm in the middle of a non-secure call and decide the call should be secure, how easy is it to change to secure mode?**

If you originally placed a call in regular (non-secure) mode, you will have to end that call and place your phone in the secure mode by entering the party's secure *data* telephone number, selecting "Secure Voice" from the user menu and pressing the SEND key.

### **6.5 How good is the voice quality of a secure call? What about delay time?**

Sectéra Wireless phones use technology that results in toll quality voice (the same as a standard wireline phone call) without detectable degradation — a superior design when compared to older-technology secure wireless devices. Delay time for regular (non-secure) wireless calls averages around .5 seconds, whereas delay time for secure calls is less than 1 second, which is considered the best among available products.

### **6.6 How long does it take to get a secure call connected?**

The average call setup times range between 15 and 40 seconds. This allows the Secure Module to exchange secure call setup information with the remote phone.

### **6.7 I am based in the U.S. — what do I need to do before I travel abroad?**

In order to use your Sectéra Wireless phone when you travel abroad, you will need to call your [GSM](#) Service Provider's Customer Care operation and request that an "International Roaming feature" be added to your account, if you do not already have it. You will also need to find out if they

## Frequently Asked Questions

have roaming arrangements with GSM Service Providers at your travel destination. In addition, you should confirm that the destination GSM Service Provider offers the necessary circuit switched data services (see [5.2](#)). The 1900 MHz frequency band is supported in North America, so your phone will need to be set to the correct frequency (900/1800 MHz) when you arrive at your destination. To change your phone's frequency, go to the "Settings" menu, select "Other Settings", select "Network", select "Network Setup" and then select the appropriate band.

### **6.8 How is my Secure Module PIN assigned?**

There is an "Encryption Management" menu that allows you to assign and modify your Secure Module [PIN](#). To make or receive secure calls, the PIN will need to be entered. The PIN is disabled when the Secure Module is powered down, which can be accomplished by powering down the phone or by removing the Secure Module from the phone. The PIN can also be disabled through the user menu.

### **6.9 How do I upgrade my phone as new functionality becomes available?**

Software upgrades can be shipped via CD-ROM, downloaded from the government website [www.securephone.net](http://www.securephone.net) or downloaded from the TalkSECURE portal. With a software upgrade cable you can upload new revisions of software from your computer to your Sectéra Wireless phone. The software upgrade cable is available for purchase from General Dynamics C4 Systems. The cable can be purchased by calling 1-781-455-2800 or toll-free at 888-TYPE-1-4-U (888-897-3148).

### **6.10 What should I do if I am not successful in making a secure call?**

Like all wireless systems, call completion is based on numerous factors including signal strength (which could mean that you are not in a coverage area or in a fringe coverage area) and battery level. These dynamic factors could prevent a secure call from being completed at any given time or place. Typically, if you are able to complete a regular (non-secure) call, you should be able to complete a secure call. If that is the case, you should try to make the secure call again.

## Frequently Asked Questions

### 6.11 What if the “Secure Voice” option is not displayed on the Dialing or Phonebook Menu option when I try to make a secure call?

If the Secure Module is removed from the phone *after* the phone was powered on, the secure menu functions will not be displayed. To correct this, recycle power by turning the phone off and then back on.

## 7. What security procedures do I need to use with Sectéra Wireless phones?

### 7.1 What do I do if my Sectéra Wireless phone is lost or stolen?

The phone and secure module are capable of three modes of security:

- 1. Uncontrolled** — a [PIN](#) is not required and it is possible for anyone to make a secure call and make changes to security settings.
- 2. Controlled** — a PIN is required and the user must know the PIN to make secure calls or change security settings.
- 3. Restricted** — a PIN is required and a Master User is also defined. The user must know the PIN to make secure calls, but only the Master User can change security settings.

It is recommended that Sectéra Wireless phones be set to Controlled or Restricted mode so that the phone is less likely to be compromised. Users are responsible for their lost or stolen [Type 1](#) Sectéra Secure Wireless phones and should report a loss through proper channels, such as their COMSEC Custodian or Supply Account manager. The user should also contact their [GSM](#) Service Provider to suspend their wireless service.

**Note:** these security modes also apply to Sectéra Wireline terminals.

### 7.2 If my Sectéra Wireless phone is lost or stolen, will someone else be able to use it to make a secure call?

When the Secure Module is filled with a [Type 1](#) key, it forces the user to create a PIN, thus forcing the phone into Controlled or Restricted mode (see [7.1](#)). Thus, the person who stole or found your Sectéra Wireless phone would also need to know your PIN to make or receive a secure call. This is similar to the situation where you have a lost or stolen ATM/Debit card. For Type 1 security, key management is part of the U.S. Government Electronic Key Management System ([EKMS](#)). This system handles distribution and revocation of keys. A Compromised Key List (CKL) is a way that the EKMS system has of identifying keys that have been compromised (lost or stolen) and disabling them so other devices

## **Frequently Asked Questions**

cannot communicate with them. This is handled by the EKMS and is transparent to the user. Also see [7.1](#) for information on reporting a stolen phone.

### **7.3 What other security procedures do I need to be aware of to use these products?**

You should consult your local security authority for security procedures applicable to the control and use of Sectéra Wireless and Wireline products.

## **8. What are some other common questions about the operation of Sectéra Wireline Terminals?**

### **8.1. Does each user need a Sectéra Wireline Terminal assigned to them?**

Each Sectéra Wireline Terminal accommodates 2 users and 1 administrator. Therefore, in cases where continuous or frequent use is not needed, you can have a “pool” of Sectéra Wireline Terminals that are controlled by an administrator and signed out on an “as needed” basis.

### **8.2. My office telephone system is digital, not analog. Will I be able to use Sectéra Wireline Terminals at the office as well as at home?**

The Sectéra Wireline Terminals only work with analog (2 wire) telephone lines, which are normally found in residential homes. Many office telephone systems are digital. In certain digital switch systems, such as Nortel, the switch provider offers analog adapters that can be used between Sectéra Wireline Terminals and the digital phone. Alternatively, most telecommunications departments can run a separate analog line to key locations where security is required. Note that the mechanical and electrical interface between Sectéra Wireline Terminals and the telephone system is exactly the same interface you would need for a phone line for your computer modem operating at 56 KBS or lower.

## Frequently Asked Questions

### Glossary

**AES:** Advanced Encryption Standard, the current encryption standard available from NIST (National Institute of Standards and Technology). The Department of Commerce approved AES as FIPS-197 (Federal Information Processing Standard) in 2002, making AES compulsory and binding on Federal agencies for the protection of sensitive, unclassified information. AES replaces Data Encryption Standard (DES), which had been developed in the 1970s.

**APK:** Automatic Public Key, General Dynamics' proprietary key management system used by Sectéra TalkSECURE products that generates and exchanges unique 128-bit session keys for every call.

**CDMA:** Code Division Multiple Access, another widespread wireless technology used by network operators worldwide.

**CO:** Central Office, a large switching center owned and operated by a telephone company, used to route telephone calls.

**FNBTD:** Future Narrow Band Digital Terminal (see [SCIP](#))

**GSM®:** Global System for Mobile Communications, the most widely deployed wireless technology.

**EKMS:** Electronic Key Management System, a U.S. Government system for ordering, generation, delivery, loading, destruction, compromise recovery and accounting of Type I cryptographic keys.

**ISDN:** Integrated Services Digital Network, an international standard for end-to-end digital transmission of voice, data, and signaling.

**Local Loop:** The wiring that connects a wireline subscriber to a CO (e.g. the wiring that comes to your home).

**PBX:** Private Branch Exchange, a local small-to-medium scale telephone switch usually located at a company's premises. For example, most hotels have a local PBX to handle all the different rooms, and guests usually dial "9" to obtain an "outside" line ("outside" the PBX).

**PIN:** Personal Identification Number, a 7-digit number that must be entered into the Secure Module before secure mode can be initiated, that allows the user to protect their wireless phone from unauthorized use.

**PSTN:** Public Switched Telephone Network, the entire public telephone system including COs, long distance carriers and local loops.

**SIM:** Subscriber Identity Module, a "smart card" which contains a computer chip and is required for all GSM wireless phones. The SIM is used to store information about a user's authentication: storage of personal data, such as speed dial and phonebook numbers; the user's PIN and information about the services ordered by the subscriber, such as voicemail. The SIM is placed in the recess behind the battery compartment in the GSM wireless phone.

**Sectéra® Architecture:** A General Dynamics C4 Systems architecture based on the SCIP signaling plan to provide interoperable secure communications. The Sectéra family of products includes the Sectéra Secure Wireless Phone for GSM (Type 1), the Sectéra Wireline Terminal (Type 1), BDI Terminal (Type 1), vIPer (Type 1), SME PED (Type 1), TalkSECURE Wireless Phone, TalkSECURE Wireline terminal, TalkSECURE Digital and TalkSECURE vIPer.

**SCIP:** Secure Communication Interoperability Protocol, a standard and a signaling scheme, which allows users to communicate securely with other compatible products.

**STE:** Secure Terminal Equipment, a component of secure voice and data equipment for advanced digital communications networks, such as Integrated Services Digital Network (ISDN). STE's provide STU-III mode and may also provide SCIP mode of operation.

**STU-III:** The STU-III is a Secure Telephone Unit that is approximately the size of a conventional telephone desk set and provides Type 1 encryption for secure classified information as well as sensitive unclassified information. The first generation STU-I was launched in 1970, followed by the STU-II in 1975 and the STU-III in 1987.

## Sectéra® Wireless and Wireline Products

### Frequently Asked Questions

**TalkSECURE™:** General Dynamics C4 Systems' high assurance secure wireless and wireline products, which have been designed to the same hardware and software architecture as Type I, but with cryptography and key management appropriate for commercial, industrial, and foreign/exportable applications.

**Type 1:** A term for processes managed by the National Security Agency (NSA) that provide approved U.S. Government users with cryptographic products and systems that are suitable for the protection of classified information.

**3G:** Third generation wireless technology designed to provide higher speed mobile access to Internet-based services, including video conferencing.

©2008 General Dynamics. All Rights Reserved.