

## **Sectéra® Edge™ Smartphone (SME PED) Frequently Asked Questions**

### **What is the Sectéra Edge?**

*The Sectéra Edge is the first and only NSA certified smartphone to provide secure wireless access to classified e-mail and websites on the government's SIPRNET (Secret Internet Protocol Router Network) as well as secure voice using commercial broadband (3G) cellular networks. The Edge can also be used to access the government's sensitive but unclassified NIPRNET network. With one touch, users can easily switch between classified and unclassified data on the device. The Edge smartphone can also be used for both classified and unclassified wireless phone calls. The Sectéra Edge was developed under the National Security Agency's Secure Mobile Environment Portable Electronic Device (SME PED) Program. It is currently the first and only NSA certified SME PED Device available today.*

### **1. How does the Sectéra Edge compare to commercial smartphones?**

The Sectéra Edge combines the features and COTS platform of a commercial smartphone with reliable Type 1 security and rugged packaging for government users. This combination reduces the total cost of ownership by minimizing user training and maximizing user uptime. Implementing Type 1 and Non-Type 1 encryption, the Sectéra Edge provides maximum flexibility in secure communications. The Edge provides these additional features:

- Type 1/Non Type 1 Secure Voice
- Type 1 Instant Messaging
- "Push" Classified Email
- Access to SIPRNET/NIPRNET
- Modem Application for SCIP Secure Data
- Interchangeable Wireless Modules
- SCIP Interoperability
- Synchronization with Classified Desktop Computer
- Type 1/Non-Type 1 DAR
- Military Grade Ruggedization
- SCIF Friendly Mode
- Integrated CAC Reader

### **2. Who are the end users of this product?**

U.S. DoD, government agencies, Homeland Security and coalition partners requiring Type 1 or Non-Type 1 security for voice and data communications. The portable form factor and remote capability makes the Sectéra Edge ideal for users on-the-move.

### **3. What are some typical applications I will use the Sectéra Edge for?**

Secure voice conversations and data applications such as secure e-mail, web browsing, viewing attachments, and access to the government's SIPRNET and NIPRNET. The secure wireless remote access capability of the Sectéra Edge allows users to replace multiple devices currently required for the same functionality. These devices include:

1. Laptop with encryptor for access to classified information on the SIPRNET

# GENERAL DYNAMICS

## C4 Systems

2. Smartphone/wireless PDA for accessing unclassified information
3. Secure cell phone for classified and unclassified phone calls

#### 4. What accessories are provided with the Edge?

The Edge comes with the GSM or CDMA wireless module, a stylus, standard battery and an AC charger.

#### 5. What optional accessories are available for the Edge?

Below is a list of accessories available. A full list can be found online at:

[www.gdc4s.com/secteraedge](http://www.gdc4s.com/secteraedge)

- Spare battery
- Extended battery
- Spare AC charger
- Vehicle DC charger
- International (UK, EU, AU/NZ) chargers
- Desktop charger
- GSM and CDMA spare wireless modules
- Classified and unclassified USB cables and adapters
- DTD and KSD Fill cables
- Software Update / Data cable
- Leather and nylon belt-clip holsters
- Executive Carrying Case
- Hands-free earbud
- Stereo headset
- 2GB MicroSD card for unclassified memory expansion
- Spare stylus 10-pack
- Privacy Screen 4-pack
- Apriva Sensa client software
- Apriva Sensa annual client rights fee
- Apriva Sensa Management and E-mail server software
- Apriva Sensa annual server software maintenance
- Apriva Sensa Installation and Training (CONUS and OCONUS)
- Edge w/o wireless module
- Wi-Fi Module
- Warranty extensions
- Executive Kits
- Desktop Kits
- Software Update Kits

**Features and Benefits**

**6. What are some of the features of this product?**

| Feature  | Benefit  |
|--|--|
| Portable, handheld form factor   | Easily transportable when on-the-move  |
| Designed to meet MIL-STD 810F specifications to withstand multiple drops, random vibrations, water, dust and can be stored and operated in extreme temperatures, humidity and altitudes. | Reliability in tactical and harsh environments as well as everyday wear and tear protects your equipment investment and maximizes user uptime.   |
| Microsoft® Windows® Operating System   | Familiar platform requires less training   |
| QWERTY keyboard with phone dial pad  | Fast and easy key typing   |
| High resolution color touch-screen display with adjustable backlight   | Easy to read text, images that can be viewed at-a-glance   |
| Wireless e-mail  | Convert downtime to productive time while on-the-move and increase responsiveness to time-sensitive decisions. Enables ability for users to access classified email while out of the office.   |
| Classified, unclassified and non-secure voice  | Classified and Sensitive But Unclassified (SBU) conversations aren't limited to the office, improves productivity  |
| COTS applications including personal organizer (calendar, contacts, tasks, alarms and notes)   | Keeps you organized wherever you are   |
| Desktop synchronization  | Keeps you up-to-date while mobile  |
| Highest-speed broadband access over GSM and CDMA cellular networks   | Fastest mobility available, both domestic and abroad   |
| Interchangeable wireless communication modules for GSM, CDMA and Wi-Fi   | Protects your core secure device investment when network requirements change   |
| Classified, unclassified and non-secure wireless e-mail & web browsing via Internet, SIPRNET and NIPRNET   | Email & web-based applications not limited to the office, improves productivity  |
| SCIP and HAIPE® IS Standards   | Instant interoperability with fielded secure devices   |
| Type 1 and Non-Type 1 encryption   | Supports cross-domain applications   |
| Integrated Common Access Card (CAC)  | Interfaces with DoD PKI for SBU applications without carrying a separate CAC reader  |
| microSD Card   | Ability to expand memory for user data storage   |
| Type 1 and Advance Encryption Standard (AES) Encrypted data-at-rest  | Protects classified and unclassified data stored on the Sectéra Edge   |
| SCIF Friendly  | With a press of a button, transmit and receive functions can be 'turned off' to enable use in a SCIF when policy allows. In "SCIF Friendly" mode, all transmitters and receivers in the device are shut down while still allowing the user to access the |

|  |  |
|--|--|
|  | PDA functions like checking previously downloaded email and viewing documents. |
|--|--|

**7. What software will be provided on the Sectéra Edge?**

- Secure and non-secure phone application
- Secure and non-secure wireless email
- Internet Explorer® web browser for access to secure and non-secure web-based applications
- Personal Organizer for secure and non-secure calendar, contacts, notes, tasks and alarms
- Windows Viewers for Images, Word®, Excel®, PowerPoint® and PDF documents
- WordPad Editor for typing secure and non-secure notes
- Instant Messenger (Classified PDA only)
- SMS for non-secure text messaging
- Windows Media® Player for full multimedia capability
- Calculator for basic mathematical operations

**8. How are classified and unclassified applications separated on the Sectéra Edge?**

The Sectéra Edge combines two (classified and unclassified) PDAs into one device. You can easily switch between the two PDAs with a single keystroke. Type 1 encryption is used for classified applications and AES encryption is used for SBU information.

**Infrastructure****9. What infrastructure is required to access my classified or unclassified e-mail?**

The infrastructure required is very similar to that required for a Blackberry implementation.

- Sectéra Edge
- Wireless cellular network service
- Connectivity to the government MCEP (Multi-Carrier Entry Point)
- Apriva Sensa Management and E-mail server software for classified and/or unclassified enclave Microsoft Exchange Server

**10. What networks does the Sectéra Edge operate on?**

The Sectéra Edge is able to adapt to a wide variety of commercial and cellular networks including commercial GSM and CDMA cellular networks worldwide as well as wireless LAN 802.11. The modular architecture allows for connectivity to wireless protocols in future enhancements and can be scaled to meet coalition demands.

Currently the Edge is certified on AT&T, T-Mobile and Verizon Wireless networks.

Other network certifications are being reviewed.

### **11. What data rates does the Sectéra Edge support?**

Data rates are consistent with commercial wireless smartphones operating on terrestrial 3G cellular networks including GPRS (216 Kb/s), Edge (216 Kb/s), UMTS (HSDPA) (downlinks up to 3.6 Mb/s) and EV-DO Rev A (downlinks up to 3.1 Mb/s)

### **Security**

### **12. What secure technology standards will be incorporated in the Sectéra Edge?**

Secure Communications Interoperability Protocol (SCIP) for secure voice and High Assurance Internet Protocol Encryptor Interoperability Specification (HAiPE® IS) for secure high-speed packet data such as e-mail and web-based applications.

### **13. What other secure voice devices will the General Dynamics Sectéra Edge interoperate with?**

Secure interoperable voice is available with hundreds of thousands of deployed SCIP devices including the Sectéra GSM Phone, Sectéra Wireline Terminal and the Sectéra vIPer™ Phone.

### **14. How will my conversations be protected?**

Sectéra Edge is NSA certified for voice information classified Top Secret and below. Data-at-rest storage and data-in-transit is certified for Secret and below.

### **15. If my Sectéra Edge is compromised, how will my stored files be secured?**

Classified files are always stored using NSA-approved file encryption, preventing compromise of critical data in the event of loss.

### **16. How is the Sectéra Edge compliant with DoD Directive 8100.2?**

DoD Directive 8100.2 establishes policy for use of commercial wireless devices capable of storing, processing or transmitting information and promotes joint interoperability using open standards. The Sectéra Edge meets requirement for data authentication, non-repudiation and personal identification for access to a DoD Information System. The Sectéra Edge also meets requirements for unclassified information, including end-to-end FIPS 140-2 encryption of unclassified data for transmission to and from wireless devices, voice encryption and FIPS 140-2 file encryption for data-at-rest (DAR). In addition, the Sectéra Edge meets requirements for classified information, including NSA-approved encryption for transmitted and stored data.

### **17. How does the Sectéra Edge use a Common Access Card (CAC)?**

CACs contain Public Key Infrastructure (PKI) digital certificates that allow you to digitally sign and encrypt SBU e-mail messages. PKI allows users of an unsecured network, such as the Internet or NIPRNET, to securely and privately exchange data. The CAC provides access to sensitive data on government networks and is used to

## **GENERAL DYNAMICS**

C4 Systems

access Non-Type 1 encrypted data-at-rest on the Edge unclassified PDA. The CAC can also be used for access control for all of the above features. If your policy allows, you can use a soft certificate instead of a CAC.

### **18. Can I use the Sectéra Edge in a SCIF?**

The Sectéra Edge is designed with a NSA-approved “SCIF-Friendly” function to easily turn off wireless capability when entering a SCIF by pressing a key.

### **Availability**

### **19. What is the price?**

The price of the Sectéra Edge is \$3,150 with a 1 year warranty or \$3,350 for a 2 year warranty. This includes either a CDMA or GSM wireless module.

### **20. When will the General Dynamics Sectéra Edge be available?**

The Sectéra Edge is NSA certified and shipping today.

### **21. How much does the monthly wireless service for the Sectéra Edge cost?**

The initial Sectéra Edge release is targeted for commercial terrestrial cellular networks. Network access and data transmission costs are determined by the commercial carriers, who typically offer various plans based on either minutes of voice service or bytes of data throughput. Sectéra Edge operational costs are consistent with commercial wireless smartphone operational costs.

### **22. How can I order the Sectéra Edge?**

The Sectéra Edge is available for direct sale and on the NSA IDIQ contract. [Ordering Information](#)

***For more information, please contact:***

## **GENERAL DYNAMICS**

C4 Systems

INFOSEC 77 A Street • Needham, MA 02494-2806 USA

Phone: 781-455-2800 • Toll-free: 888-Type1-4U (888-897-3148) • Fax: 781-455-5555

Email: [infosec@gdc4s.com](mailto:infosec@gdc4s.com) • Web Site: [www.gdc4s.com/secureproducts](http://www.gdc4s.com/secureproducts)

© 2009 General Dynamics. All Rights Reserved. Sectéra, Edge and vIPer are trademarks of General Dynamics. HAIPE is a trademark of the National Security Agency. All other product and service names are the property of their respective owners. ® Reg. U.S. Pat. & Tm. Off. General Dynamics reserves the right to make changes in its products and specifications at anytime and without notice.