KG-201

External Hardware Encryptor to Protect Mobile Classified Data at Rest

When disaster strikes, the ViaSat KG-201 Inline Media Encryptor (IME) foils threats to national security. Developed and certified by the NSA, the KG-201 is the first and only mobile media encryptor that protects classified Data at Rest (DAR) at Top Secret (TS/SCI) and below. In the event that a classified laptop, notebook or other mobile computer is lost, stolen or tampered with, its hard drive remains encrypted. Simply remove the KG-201's Cryptographic Ignition Key (CIK) to quickly secure the hard drive and eliminate the need to handle it as a classified device.

For added convenience and portability, the KG-201 is able to house your laptop's hard drive or act as an external hard drive for secure mobile and transportable data storage. It's also small enough to fit in the palm of your hand and easily connects to any brand of commercial-off-the-shelf (COTS) PC via USB. In the event you need more secure data storage in the future, simply replace the hard drive housed inside your KG-201 with a COTS hard drive of larger capacity.

Protect your mobile DAR with simple Type 1 encryption from ViaSat's family of IMEs.

APPLICATIONS—HOW THE KG-201 CAN HELP YOU

- Classified DAR Compliance (J-6 6510.01E directive)
- Laptop and Mobile Computer Users
- Improve Accountability when Hand-Carrying Data from Location to Location
- Control Access to Stored Classified Data without Impeding Operations
- Remote Military Outposts
- Eliminate Need for Classified Network
- Semi-Rugged for Use in the Field
- SCIFs and Embassies
- Easier DAR Storage and Transportation

TS/SCI DAR ENCRYPTION FOR LAPTOPS

EASY TO USE, STORE, AND TRANSPORT

- Fits in the palm of your hand and weighs just 1.5 lbs with drive
- Universal USB 2.0 connection
- Encryption eliminates classified data storage and transportation requirements
  - Encrypted hard drive is always unclassified—No need to lock it up in a safe!
  - Just remove the CIK to handle the KG-201 as an unclassified CCI device
- To operate, simply connect to your PC, insert the CIK, enter the 4 digit PIN, and you're ready to go!
- Transparently encrypts and decrypts data written to and read from the computer's drive as information is accessed by the user
- Continuous hard drive encryption operates in real-time without slowing down the computer's processing speed
- Supports up to ten user accounts

MEETS SECURITY STANDARDS

- NSA Certified for TS/SCI and below data
- Two-factor authentication–requires a CIK ("something you have") and PIN ("something you know") for access
- Provides Emergency Data Destruction without destroying equipment or losing data
- Meets NSA's Crypto Modernization Initiative (CMI) and Key Management Infrastructure (KMI) standards

INTELLIGENT KEY MANAGEMENT

- CIK renders device unclassified when removed
- Self-generating storage key; no key distribution required
- In the case of zeroization, mechanisms are in place for data recovery and retrieval

HARDWARE AND SOFTWARE INDEPENDENT

- Delivered with 110 GB hard drive installed; or, pick your own size of hard drive or solid state drive tailored to your mission
- Compatible with all standard operating systems including Microsoft® Windows® 2000/XP/Vista/7, Linux®, and Apple® Mac OS® X

AVAILABLE TODAY

- The KG-201 is already NSA certified and available for use now

External Hardware Encryptor to Protect Mobile Classified Data at Rest

SPECIFICATIONS

KG-201 INTERFACES

Electrical/Mechanical Connection via USB 2.0 to any COTS computer
Throughput Speed 480 Mbps
Internal Hard Drive ATA-6/Ultra ATA-100, supports standard 2.5-inch COTS laptop drive sizes
Power Supplied by 5 VDC wall adapter, optional battery, or other sources

SECURITY CHARACTERISTICS

Algorithms Protects Data TS/SCI and Below using AES-256 Type 1 Suite B
Flexibility Modular, reprogrammable architecture
Crypto Ignition Key CIK Removal to Unclassified CCI
Emergency Zeroization Meets requirements for rapid zeroization
Tamper Protected

PHYSICAL

Dimensions (WxHxD) 3.5 x 1.75 x 5.7 in
Weight 1.5 lbs (including typical hard drive)

RELIABILITY AND MAINTENANCE

Predicted MTBF 66,000 hours ground benign
Predicted MTTR Five minutes mean time to replace
Built In Test Power up bit
Software/Firmware Updates Field upgradeable

ENVIRONMENT

Operating Temperature -29°C to 55°C
Storage Temperature -29°C to 70°C
Humidity Up to 90% (Non-Condensing)
Shock 20G 11 ms
Vibration 9G RMS 5-2000Hz

CERTIFICATION

NSA Type 1 Certified for TS/SCI and below
TEMPEST Compliant NSTISSAM 1/92

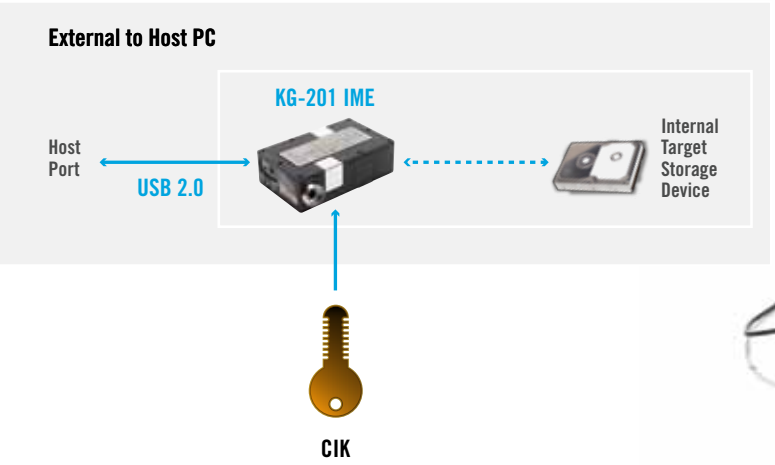
CUSTOMIZATION

Variations in interfaces, functionality, ruggedness, and form factor can be customized to suit your specific requirements. Contact ViaSat to discuss your DAR protection requirements.

TRUSTED SUPPORT

1-year warranty included; optional multi-year warranty available.
Free training and 24/7 technical support.

HOUSES CLASSIFIED HARD DRIVE AND CONNECTS TO ANY COTS LAPTOP VIA USB



CONTACT

6155 EL CAMINO REAL, CARLSBAD, CA 92009

SALES
TEL 888.VIASAT.1 (888.842.7281) **FAX** 760.683.6815 **EMAIL** INSIDESALES@VIASAT.COM

TECHNICAL SUPPORT
TEL 760.476.4754 OR 888.VIASAT.4 **FAX** 760.929.3938 **EMAIL** ALTASEC@VIASAT.COM **WEB** WWW.VIASAT.COM/SECURE

Copyright © 2011 ViaSat, Inc. All rights reserved. ViaSat and the ViaSat logo are registered trademarks of ViaSat, Inc. Microsoft and Windows are registered trademarks of Microsoft Corporation. Linux is a registered trademark of Linus Torvalds. Apple and Mac OS are registered trademarks of Apple Inc. All other trademarks mentioned are the sole property of their respective companies. Specifications and product availability are subject to change without notice. Version 1 of ATA was commonly known as Integrated Drive Electronics (IDE). The Type 1 encryption provided by this product is part of the Department of Defense "Defense In Depth" strategy. Type 1 encryption is only one portion of the overall defense in depth. A comprehensive network Information Assurance strategy involving "Defense In Depth" is required to ensure secure and reliable protection for sensitive and classified information.