ECTOCRYP® Black is a high-capacity programmable, secure, voice encryption device that can protect voice communications up to and including Top Secret. NSA-approved to operate, tested by JRTC and listed on DISA's approved product list as a DoD Secure Communications Device, it is now available to U.S. government customers, providing multi-channel encryption between red enclaves and remote Secure Communications Interoperability Protocol (SCIP) devices. For example, numerous simultaneous callers using SCIP terminals such as Sectera vIPer, Omni, etc., on an unclassified network can speak securely to users on normal telephones within a red or classified enclave via a single ECTOCRYP® Black gateway device. Additionally, on multilevel secure voice networks (DRSN), it can be configured to interoperate with multilevel secure voice switches.

For more information please visit www.ECTOCRYPBlack.com.

**Benefits**

- **Interoperability:** Its open-standards design allows ECTOCRYP® Black to be used with media gateways to allow SCIP-compliant encryption and decryption of both Time Division Multiplexing (TDM) and Internet Protocol (IP) secure voice devices.
- **Convergence:** Multiple encryption keys can be resident to accommodate multiple communities of interest, facilitating communication from multiple sources. Enterprise services, such as teleconferencing, can also be enabled.
- **Efficiency:** Allows installations with high volumes of secure voice communications to meet their needs with a single device, potentially at lower cost than traditional means.
- **Extensible:** Multiple ECTOCRYP® Black units can be used in parallel to add capacity in blocks of 92 users each.
- **Adaptable:** As a programmable cryptographic unit, ECTOCRYP® Black can be modified to incorporate new standards or additional features to meet evolving customer needs such as VoIP, new SCIP versions, or different algorithms.
Applications

- Secure voice communications stream at Maritime Operations Centers, Air Operations Centers, Tactical Operations Centers and Headquarters secure enclaves as an interface via unclassified telephone networks
- Interface with the Multilevel Secure Voice network to add capacity with a smaller footprint and lower cost than legacy equipment Installations that enable secure voice enterprise solutions, satellite ground station encryption of voice communications, and encryption of voice communications for multiple types of red enclaves

Technical Specifications

Management Support via Laptop

- Local Management via 100 Base-T connectivity
- Windows hosted custom management application
- SNMP v3 compliant management capability
- Supports management via front and rear management ports (IPv4)
- ECTOCRYP® Black can be configured for either E1 or T1 operation via the management console
- ISDN Link status can be viewed via the management console.

Protocol Support

- SCIP
- QSIG
- Ni2

Cryptography Support

- Field Programmable Gate Array design provides flexibility with programmable architectures
- Capable of protecting TOP SECRET, including national caveats
- Over 250 keys may be stored simultaneously. Compatible with DS 101 key loaders
- Designed to support EKMS 308 and 319
- Records COMSEC accounting events and general accounting events
- Supports full upload of the accounting records

Capacity

- Up to 120 simultaneous secure voice calls in E1 configuration or 92 in T1
- Can receive input from four T1 or E1 lines

Physical Interfaces

- Management — 100-Base-T interface (RJ45 Connectors front and rear)
- RED — 4 x E1 or T1
- BLACK — 4 x E1 or T1
- Power – AC input 85 to 264v (47 to 63Hz)

Upgradeability

- Fully in-field reprogrammable, from protocol handling to cryptographic algorithm suites
- Fully upgradeable to VoIP/SIP (future feature, v.150 gateways used now)
- Conferencing (future feature, standard call managers can be used now)
- Adding crypto modes for NATO and other standards is possible

Certification Features

- NSA-approved to operate up to Top Secret
- SCIP compliance tested
- JITC evaluated, listed on DISA’s UC APL
- Designed for NATO SDIP-27 A (formerly AMSG 7206) Tempest accreditation
- UL approved

Physical Specifications

- 6U 19" rack mountable (10.5”H x 19”W x 20”D)
- Weight — 66 lbs
- Operating temperature 32° to 104°F — Humidity <90% non-condensing
- Storage temperature -4°F to 140°F — Humidity <90% non-condensing

Interoperability

- Designed to be fully interoperable with SCIP devices (e.g., Sectéra® SMax™, Omni, etc.)
- JItC-tested for DSN and DFRSN

Security Features

- Crypto Ignition Key (CIK) dramatically reduces cryptographic distribution, handling and accounting
- Tamper resistant
- Full erase functionality
- Delivered as UNCLASSIFIED CCI

Special Features

- Secure dialing for menu options
- Dialed number translation
- Both DSN and DFRSN configurations resident
- Accommodates vocoder rates as low as 2400bps
- Records call details to a call log within the unit
- Active calls can be viewed via the management console
- Supports full call log upload from the unit in .csv format

Provided per Government contract

- One ECTOCRYP® Black encryption device
- Two voice interface cards (one each for Red and Black sides)
- Power distribution panel & ancillary cables/connectors
- One-year standard warranty (extended warranties available)
- Software (operating, manuals, user guide, etc.)