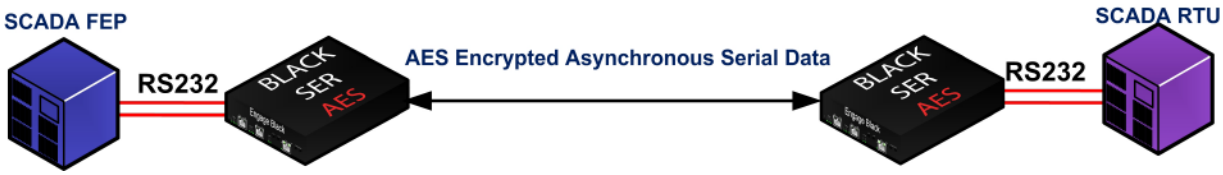
ENGAGE BLACK

Black•Ser AES

Serial Encryptor

The **Black•Ser AES** is an in-line Serial Data Encryptor with FIPS 140-2 Level 3 certified cryptography and hardware. Serial data received on the DCE interface is encrypted using a 256 bit AES key and sent out the DTE interface. Serial data received on the DTE interface is decrypted using an 256 bit AES key and sent out the DCE interface.



256 bit AES encryption key can be internally generated or imported with key wrapping

Seamless Integration

Retrofit existing serial communications systems easily with the **Black•Ser AES's** simple bump-in-the-wire design protects: meters, protective relays, programmable logic controllers (PLCs), remote terminal units (RTUs), and computers from unauthorized access, control, eavesdropping, and malicious attack by authenticating and encrypting all serial data communications.

The **Black•Ser AES** securely boots up as a protocol agnostic asynchronous Serial Data Encryptor executing inside of a tamper reactive cryptographic boundary. All cryptographic functions, including private and public key generation are performed inside FIPS Level 3 protected hardware. The cryptographic algorithms are FIPS certified. Internally generated keys use a NIST certified hardware seeded random number generator to ensure key entropy.

Military Grade Tamper Reactive

Master key is secured within CPU Die Shield's Cryptographic Boundary. Dynamic fault detection with real time environmental and active tamper detection circuitry.

- Achieves Active Level 3+ Tamper
- Transport Safe

ENGAGE BLACK

Black•Ser AES

Serial Encryptor

Secure and Effective Management
Management interface is accessed by an authenticated and encrypted Secure Socket Shell channel. Operation is partitioned by privilege into security relevant functions that are Administrator, Auditor and Operator role based.

Key Management
The **Black•Ser AES** core cryptography is based upon our FIPS approved Hardware Security Module. FIPs requires a sophisticated protection private key generation, exportation and importation. Authentication of connection is able to utilize Certificates whose status is polled (OCSP).

Technical Specifications

RS232 Interfaces:
- 1 RS232 DCE (RJ45)
- 1 RS232 DTE (RJ45)
- Baud Rate:
  1.2/2.4/4.8/9.6/19.2/38.4/57.6/115.2 Kilobits

Serial Protocols Supported:
- Asynchronous 8 bit: Modbus, DNP, IEC101, etc..

LAN Network Interface:
- 1 Ethernet 10/100 BaseT Copper
- TLS

Hardware
- Hardware True Random Number Generator
- NIST SP 800-90 compliant DRBG
- Secure Boot Loader: PKI Authentication
- Memory Encryption And Integrity Check
- Real-Time Clock
- Tamper: Mechanical, Die-Shield, Temp & Voltage

Physical Characteristics
- Rack, Wall and Din Rail Mounting
- Dimensions 102 x 153 x 26 mm (4 x 6 x 1in)
- Weight: 454 grams; 1 pound
- Temperature: operating -20 to 60°C,
- Humidity: operating 10 to 90%
  storage 0 to 95%

Certification
- FIPS 140-2 Level 3

Cryptography
- Symmetric algorithm: AES 256 bit

Management and Monitoring
- Web GUI run in web browser
- Syslog diagnostics support

Safety & Environmental Compliance
- UL, CE, FCC • RoHS

Power
- DB9 Connector: Dual Hot Standby 5 to 30 VDC
- Power consumption: 4W