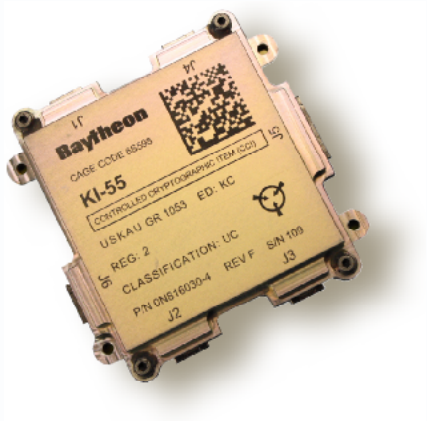
Raytheon

Gryphon AES AVE KI-55

Complete TT&C Security Solution



General-Purpose AVE for simultaneous authenticated command uplink decryption and mission/telemetry downlink encryption

Key Specifications

- Uplink Algorithm:
  - AES-256 (NIST FIPS-197) Modes: GCM, ECB, CTR, and CFB
  - Authenticated Command Modes: GCM and ECB with VCC (Vehicle Command Count)
- Downlink Encryptor Algorithm:
  - Fail-Safe Redundant AES-256 Modes: GCM, CTR, and CFB
  - Random number generator (RNG) for initial vector generation
- Over-the-Air Rekey (OTAR):
  - AES-256 ECB per KMI 3240 Key Wrap Spec
  - In-band or in-flight transferring of black key

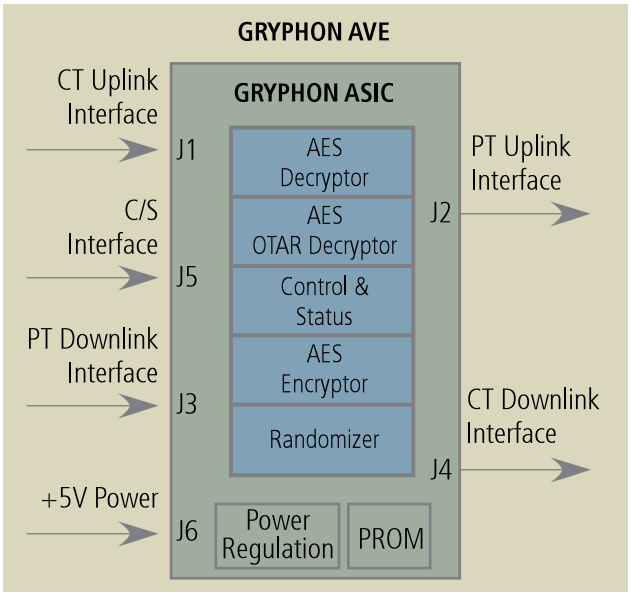
This Type 1 TT&C provides both Uplink and Downlink COMSEC protection in a single compact unit.

Features available for the first time in a space crypto solution:

- Multiple cryptographic modes and flexible synchronization logic support many mission profiles and CONOPS
- GCM cryptographic mode supports variable length authenticated commands up to 32k bytes in length
- Integrity verification downlink option is ideal for tactical applications, such as UHF radios
- Multiple authenticated command channels enable direct payload or satellite tasking from tactical and/or multiple users
- Highly integrated single chip embedded ASIC within the AVE reduces footprint and power
- Unclassified; designed for releasability

Additional Advantages:

- Protects data through TS/SCI
- Interoperable with KIV-7M, Enhanced Suite B Gryphon GOE
- Miniaturized AVE is an ideal choice for SmallSat, NanoSat, and CubeSat
- Over-the-Air Rekey (OTAR) capability to extend mission service life and allow dynamic crypto net management



KI-55 Block Diagram

Additional Specifications

Key PROM: 256 downlink keys; 224 uplink keys; 32 key encryption keys
Data Rates:
Uplink: 100 bps to 20 Mbps
Downlink: 100 bps to 20 Mbps
Operating Temperature: -24 to +61° C
Size and Weight: 3.07"L x 3.04"W x 0.65"H; 3.9 oz. (111g) max.
Power and Voltage:
Less than 1.7W (nominal)
+5VDC Primary Power
Radiation: All components qualified to 100 Krad (Si) or better
MTBF: ~250,000 hours
MIL-STD-461F (Tailored)

Subject to change without notice.

Sales/Support Inquiries:
(310) 616-1124
dana.gastelum@raytheon.com

www.raytheon.com/capabilities/cybersecurity/sis

Raytheon
Customer Success Is Our Mission