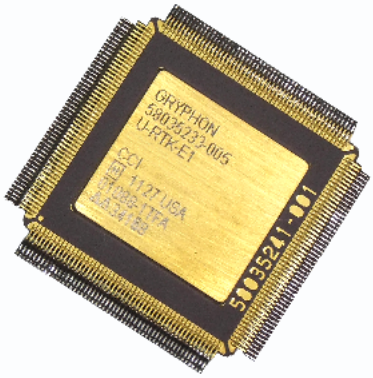
Raytheon

U-RTK Gryphon AES ASIC

NSA-Certified Fully Integrated Satellite Link Security Solution



General-Purpose, Dual Channel High Speed Embeddable Processor for Simultaneous Authenticated Command Uplink Decryption and Mission/Telemetry Downlink Encryption

Specifications

- Uplink Algorithm:
  - AES-256 (NIST FIPS-197) Modes: ECB, CTR, GCM, and CFB
  - Authenticated Command Modes: GCM and ECB with VCC (Vehicle Command Count)
- Downlink Encryptor Algorithm:
  - Fail-Safe Redundant AES-256 Modes: CTR, GCM, and CFB
  - Random number generator (RNG) for initial vector generation
- Over-the-Air Rekey (OTAR):
  - AES-256 ECB per NIST AES Key Wrap Spec
  - In-band or in-flight transferring of black key
- Interfaces:
  Traffic, Key PROM, Command, and Control
- Uplink Traffic Interface:
  Serial LVTTL clock, data, and enable
- Downlink Traffic Interface:
  - Serial LVTTL clock and data
  - 8/16-bit parallel clock and data

This Type 1 640 Mbps features low-power and Is Radiation Hardened.

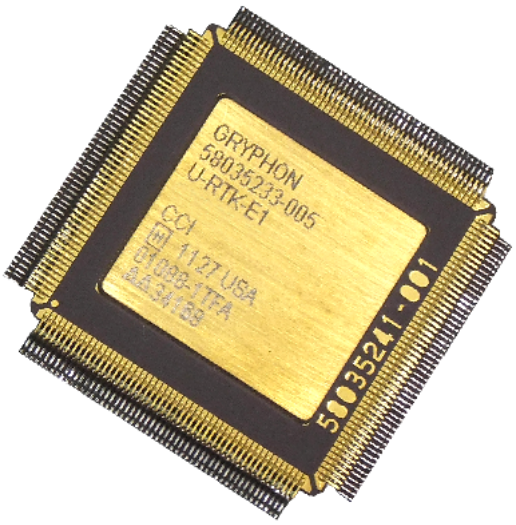
Features available for the first time in a space crypto solution:

- Multiple cryptographic modes and flexible synchronization logic support many mission profiles and CONOPS
- GCM cryptographic mode supports variable length authenticated commands up to 4k bytes in length.
- Authenticated downlink capability 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 solution for both command uplink and data downlink security reduces footprint
- Unclassified design for high risk-of-loss environments and coalition partners

Additional Advantages:

- Protects data traffic up through TS/SCI
- Interoperable with KIV-7M Enhanced Suite B Gryphon GOE
- Radiation hardened 1 MRad (Si), latch-up immune, QML-V
- Unclassified and CCI when not keyed
- Over-the-Air Rekey (OTAR) capability to extend mission service life and allow dynamic crypto net management
- Radiation hardened to support all orbits
- On-chip synchronization detection reduces need for external circuitry

U-RTK ASIC



Additional Specifications

Key PROM Interface: Adresses up to 512 keys

Data Rates:

- Uplink: 100 bps to 40 Mbps
- Downlink: 100 bps to 40 Mbps (serial), 320 Mbps (8-bit parallel) and 640 Mbps (16-bit parallel)

Operating Temperature: -55 to +125° C

Package Size: 208-pin CQFP, 29.1 x 29.1 mm^2

Power:

- Supply Voltage: +3.3VDC
- 0.2W @ 1Mbps; 0.6W @ 20 Mbps; 2.8W @ 640Mbp

Technology: 0.35 micron, SOI, 1MRad

MTBF: ~1,000,000 hours

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

www.raytheon.com/capabilities/
cybersecurity/sis

Raytheon
Customer Success Is Our Mission