

MILITARY-
GRADE
ENCRYPTION
FOR NON-TYPE 1
APPLICATIONS

Harris Citadel[®] Cryptographic Engine



KEY BENEFITS

- Military-grade encryption for non-Type 1 applications
- Rapid-state swapping
- Three unique algorithm options
- Customer configurable
- Field and analytically tested security

The Harris Citadel Cryptographic Engine provides high-grade protection for all modern communications media, enabling users to safely transmit sensitive information over normal communications channels. Available to both U.S. and international users, it is approved for export with multiple algorithm options—and it is ideal for a broad range of communications products.

Citadel comes complete with three unique algorithm options: a standard Citadel high-grade algorithm, a Harris-configured Citadel algorithm (customer unique), and a customer-configurable Citadel algorithm. With these three options, users can easily adjust their level of security without physically modifying their equipment.

Based on a mixed-mode, arithmetic block cipher, all three algorithms support both communication security and transmission security functions. Plus, each has been proven to withstand sophisticated cryptographic attacks—both analytically and in the field.

Citadel provides half-duplex encryption and decryption at throughput data rates of up to 5 Mbps. It processes serial or parallel unencrypted and encrypted data, and includes key management commands in the IC's command set to help meet varying user requirements. All interfaces are 3.3V and 5V CMOS compatible.

Delivering military-grade encryption for non-Type 1 applications, the Harris Citadel Cryptographic Engine ensures your critical communications remain secure.

HARRIS[®]
assuredcommunications[®]

Specifications for: Harris Citadel® Cryptographic Engine

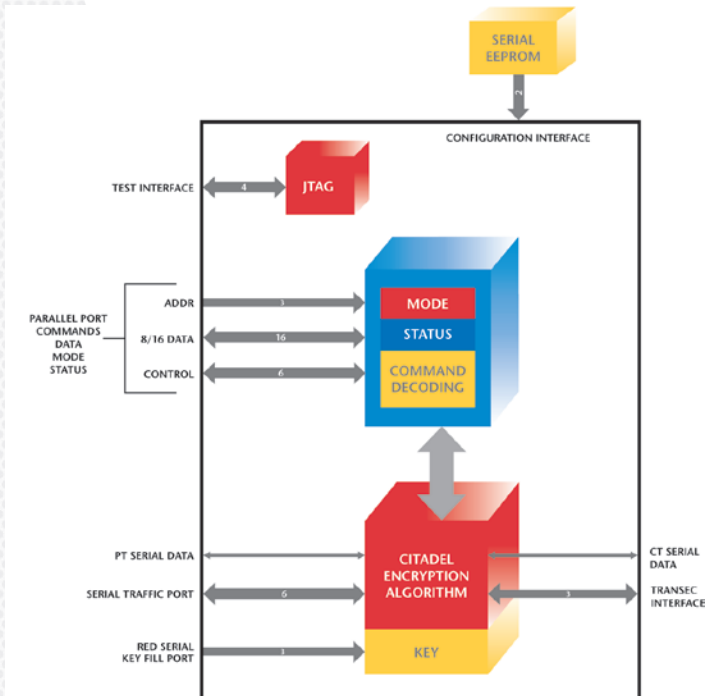


Diagram caption needed

LEARN MORE

To learn more about the Harris Citadel Cryptographic Engine and its advanced features, contact Harris at TacticalCommunications@harris.com.

Harris is dedicated to developing best-in-class *assured communications*® products, systems and services.



GENERAL

Multiple Algorithms	Standard Harris proprietary high-grade algorithm Harris-configured algorithm (customer unique) Customer-configurable unique algorithm
Cryptographic Strengths	Configurable key lengths Proven secure against differential and linear cryptanalysis Third-party verified
Multiple Cryptographic Modes	Block Cipher Feedback Self-Synchronizing Cipher Feedback Long Cycle or Minimum Error Propagation Codebook (Key processing only)
Cryptographic Keys	Traffic encryption key—minimum 1.8 x 10 ¹⁹ Key encryption key—minimum 1.8 x 10 ¹⁹
Key Management	On-chip key storage for KEKs and TEKs Key wrapping/unwrapping Key updating Deterministic key generation Non-deterministic key generation
Interface	Independent TRANSEC

TECHNICAL

Dimensions	80 pin TQFP 16 mm x 16 mm (0.63 x 0.63 in.)
Industrial Temperature	-40°C to +85°C
Data Rate	Up to 5 Mbps
Power	3.3 or 5 volt supply
Operational	3.0V (min) to 5.5V (max)

PORTS

Parallel Port	A bi-directional interface used to control the chip's operation. Commands, status, bytes and command data are passed via this port in 8- or 16-bit format. Encryption and decryption can be processed via the Parallel Port in either 8-bit or 16-bit format.
Power Port	Compatible with 5V or 3.3V DC power.
Serial Traffic Port	Contains all data and control lines necessary for encryption and decryption. PT and CT data are on different pins to provide red and black data separation.
Red Serial Key Fill Port	Load keys via this port.
Serial EEROM	Enables user-unique configuration information for the IC to be read by the Configuration Interface or loaded via the Parallel Port.
Housekeeping Port	Contains the /RESET, /ZERO, STAND_ALONE, CONFIG/DE signals.
Test Port:	Contains the Test Access Port (TAP) interface for Boundary Scan.

Harris, Citadel and *assured communications* are registered trademarks of Harris Corporation. This information was approved for all publishing per the ITAR as "basic marketing information of defense articles" or as "advertising printed material" per the EAR. Specifications are subject to change without notice. © 2015 Harris Corporation 11/15_DS-206G