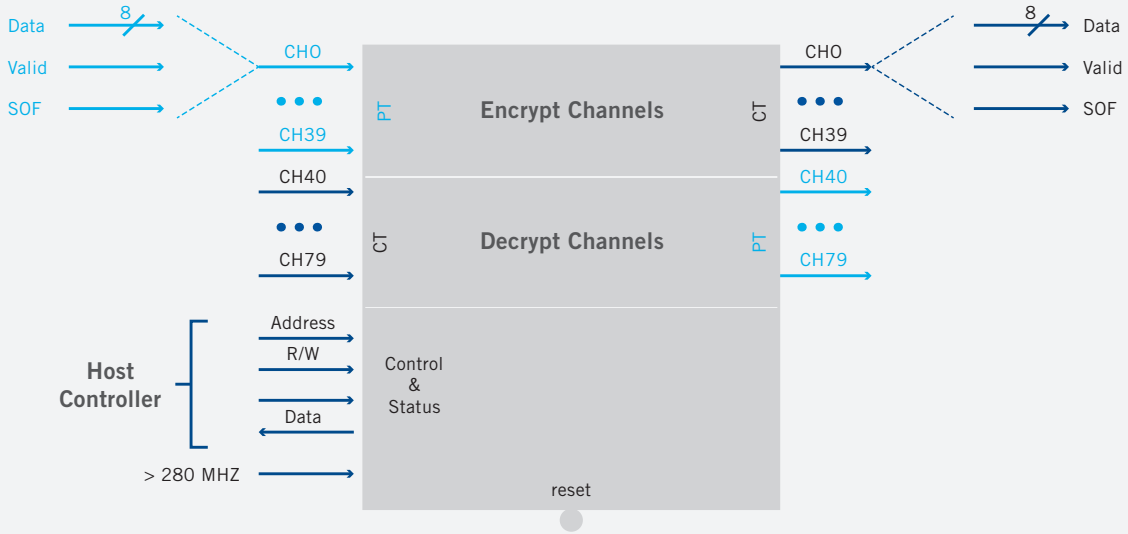
Viasat IP Core

Multi-Channel AES-256/128 Security Core

Viasat's Multi-channel 100 G Security IP core enables high-speed chip and systems designers to incorporate comprehensive high-grade security into their products with minimal integration effort. Viasat's core is much more than just an "AES algorithm" core; it is a complete security system core. The core includes a comprehensive set of already-integrated security functions which can be dropped into a customer's FPGA or ASIC design. As the core includes all the security functions, no security expertise is required of the systems integrator.

SIMPLE INTERFACE



Viasat's security core interfaces to the host system through multiple independent encrypt/decrypt data channels and a simple control and status bus. All interfaces are synchronous to the 280 MHz clock.

Viasat IP Core: Multi-channel AES-256/128 Security Core

MINIMAL HOST SUPPORT

The security core only requires a one-time configuration load after power-cycle/reset. This configuration load contains one 256/128-bit Key Encryption Key (KEK) + 32-bit CRC for each of the 80 channels. Once configured, the security core will automatically setup a secure connection to its peer core(s) in the distant-end equipment. No other configuration is necessary. The management interface also provides status information to the host indicating the status of security connection(s) as well as other link statistics.

SPECIFICATIONS

- **Data Interface** — 80 channel x 1.33 Gbps (106 Gbps aggregate)
- **Overhead** — Single byte per frame (crypto overhead channel)
- **Algorithm and Mode** — AES-256/128 encryption/decryption using counter mode
- **Cryptographic Synchronization** — Automatically established after 1 complete cryptographic frame (8 frames = 1 cryptographic frame)
- **80 Fully Independent Channels** — Each channel may have different TEK, cryptographic state, & peer authentication KEK

- **Integrated Key Management**
  - Traffic Encryption Keys (TEKs) generated using built-in non-deterministic random number generator.
  - Secure key exchange/distribution using AES key wrap.
- **Integrated Peer-to-Peer Authentication (Shared Secret Symmetric Cryptography)**
  - Peers automatically authenticate each other immediately after the cryptographic overhead channel is established.
  - After an upset event (like power loss), authentication is automatically re-established.
- **Automatic Key-Rollover and TEK Generation**
  - New random keys are generated automatically prior to crypto-midnight, and securely exchanged using the crypto overhead channel.
  - TEK roll-over is seamless and transparent to data channel (no lost data before, during, or after TEK roll-over)
- **Controlled Cryptographic Bypass for Non-Encrypted Frame Data** (Overhead bytes).

FPGA UTILIZATION (XILINX VIRTEX-6): 256-BIT KEY VERSION

COMPONENT	FFs	LUTs	BRAMs (36 k)
106 Gbps AES-256 ECB Core	17,964	39,831	—
Controlled Cryptographic Bypass	2,978	3,321	17
Data Interface Adaptor (80-CH)[1]	17,563	25,692	80
80-CH Context Ctrl w/Key Rollover	13,211	13,344	10
Key Manager & Peer Authenticator	4,429	7,433	26
Security Core Total[2]	**56,145**	**89,621**	**133**

CONTACT

SALES
TEL +1 216 706 7800 **EMAIL** ipcores@viasat.com **WEB** www.viasat.com/advanced-technology

Copyright © 2017 Viasat, Inc. All rights reserved. Viasat and the Viasat logo are registered trademarks of Viasat, Inc. All other product or company names mentioned are used for identification purposes only and may be trademarks of their respective owners. Specifications and product availability are subject to change without notice. [1]This estimate makes some assumptions about the data interfae maximum burst size and framing alignment. Actual FPGA utilization could vary (up or down) depending on the actual interface characteristics. [2]Occupied Slice utilization will vary with P&R settings, optimizations, and floor planning choices. Using typical rations: Slice-to-LUT ~ 1:2.3 and Slice-to-FF ~ 1:2.77, results in an occupied slice count of approximately 32,354 (37% of XC6VHX565). 468089-171013-004