ViaSat’s Multi-channel 100G 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 280MHz clock.
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 & 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 & 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 & 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

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>FFs</th>
<th>LUTs</th>
<th>BRAMs (36k)</th>
</tr>
</thead>
<tbody>
<tr>
<td>106 Gbps AES-256 ECB core</td>
<td>17,964</td>
<td>39,831</td>
<td>—</td>
</tr>
<tr>
<td>Controlled Cryptographic Bypass</td>
<td>2,978</td>
<td>3,321</td>
<td>17</td>
</tr>
<tr>
<td>Data Interface Adaptor (80 CH)¹</td>
<td>17,563</td>
<td>25,692</td>
<td>80</td>
</tr>
<tr>
<td>80-CH Context Ctrl w/Key Rollover</td>
<td>13,211</td>
<td>13,344</td>
<td>10</td>
</tr>
<tr>
<td>Key Manager &amp; Peer Authenticator</td>
<td>4,429</td>
<td>7,433</td>
<td>26</td>
</tr>
<tr>
<td>Security Core Total²</td>
<td>56,145</td>
<td>89,621</td>
<td>133</td>
</tr>
</tbody>
</table>

¹ This estimate makes some assumptions about the data interface 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 ratios: 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).