EIP-196: Intellectual Property (IP), family of security engines for high-speed flow-through processing of IPsec, MACsec and also look-aside acceleration of security operations

Support for cryptographic security has become a basic requirement for many networking and mobile silicon devices. This creates a challenge for semiconductor designers who realize that cryptographic security processing needs assist from dedicated hardware to achieve the levels of throughput required by today’s applications. Implementing security functionality on dedicated hardware enables designers to achieve higher throughput performance, lower power consumption, and a higher degree of security over software-based implementations running on a general-purpose processor. SafeNet offers its expertise in the design and integration of dedicated security hardware to semiconductor designers by means of its SafeXcel IP product portfolio. The SafeXcel IP Flow-Through Engine (SafeXcel-IP-196 / EIP-196) is one of SafeNet’s sophisticated, highly-integrated security modules, designed for networking applications.

High-Performance Security Processing

The SafeXcel-IP-196’s value lies in its unique capability to maximize data plane offloading from a host processor to dedicated hardware. In traditional SoC architectures, hardware assist is usually limited to modules that perform cryptographic security processing under full control of an embedded general-purpose processor. In these architectures, the general-purpose processor still needs to process each packet to some extent. Especially at high data rates and for small packet sizes, this approach creates a significant processing burden on the processor, and it may even create an overall throughput bottleneck. With the SafeXcel-IP-196 on the other hand, the general-purpose CPU is not involved in processing packets that belong to an existing data flow. This allows the CPU to dedicate its clock cycles to data flow setup and other processing tasks. The SafeXcel-IP-196 embeds the SafeXcel-IP-96 Packet Engine. The result is a high-performance security solution that delivers Gigabit rate processing.

Micro-programmed Packet Classification / Flow Processing

The SafeXcel-196 provides full data plane processing up to the IP/IPsec layer. This capability is enabled by the engine’s unique Packet Classifiers and Flow Processors and is not offered by other security IP vendors. While traditional offerings need to rely on external classification, the SafeXcel-IP-196 includes micro-programmed hardware assist for this time-consuming task. The SafeXcel-IP-196 autonomously inspects packets, determines required processing and instructs the Packet Engine which transformation to execute.

Application use cases and solutions

The SafeXcel-IP-196 is intended to be used in the following use cases:

In the look-aside use case, the EIP-196 is a co-processor in the system and is processing packets that are prepared and consumed by the host CPU. In the bump in the stack use case, the EIP-196 sits in between MAC and OS network stack and takes care about data plane processing for MACsec or IPsec. OS stack will never see encrypted packets. In the bump in the wire use case, the EIP-196 is used to process packets from one MAC to another MAC for established connections without host being involved.
Bus master
Bus slave
SPD
Control
Mem access bus mux

processing to a Soc’s inline Security engine, maximizing application performance. the toolkit also
QuickSec ipsec toolkit. the QuickSec ipsec toolkit’s advanced architecture offloads data plane
Hardware security functionality in a Soc needs to be supported by state-of-the-art software to
integrated software support is increasingly becoming a critical success factor for complex Socs.

Complete Hardware/Software Solution
Due to its capability to perform complete packet processing in hardware, at 300MHz (TSMC 90nm) the
SafeXcel-IP-196 reaches up to 1 Gbit full-duplex throughput (2 Gbit aggregate) for all packet sizes.

Performance
Integrated software support is increasingly becoming a critical success factor for complex SoCs.
Hardware security functionality in a SoC needs to be supported by state-of-the-art software to
make the SoC successful in its market. The SafeXcel-IP-196 works seamlessly with SafeNet’s leading
QuickSec IPsec toolkit. The QuickSec IPsec toolkit’s advanced architecture offloads data plane
processing to a SoC’s Inline Security Engine, maximizing application performance. The toolkit also
enforces policies upon the Packet Classifier as part of its control plane functionality.

Solutions
Look-aside Bump in the stack Bump in the wire
IPsec gateway - - +
IPsec aware EMAC - + +
MACsec aware EMAC + + +
Look-aside crypto accelerator + + +

Hardware configurations and Options
The SafeXcel-IP-196 features a modular interface design, allowing flexible integration into various
host systems. The Packet Engine is offered in 4 configurations, each with a choice of an AHB, AXI or
PLB interface. For more options, or alternate configurations of the ciphers please contact SafeNet.

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Hardware capability</th>
<th>Gate count</th>
<th>Freq. (MHz)</th>
</tr>
</thead>
<tbody>
<tr>
<td>EIP-196i</td>
<td>IPsec, MACsec, sRTP + AES-GCM/CCM/CCM/GMAC/XCBC-MAC</td>
<td>750</td>
<td>300</td>
</tr>
<tr>
<td>EIP-196ie</td>
<td>The EIP-96i + with SHA-384/512</td>
<td>790</td>
<td>300</td>
</tr>
<tr>
<td>EIP-196is</td>
<td>The EIP-96i + with SSL(D)/TLS + ARC4</td>
<td>810</td>
<td>300</td>
</tr>
<tr>
<td>EIP-196ies</td>
<td>The EIP-96i + with SSL(D)/TLS + ARC4, SHA-384/512</td>
<td>850</td>
<td>300</td>
</tr>
</tbody>
</table>

Corporate Headquarters:
4690 Millennium Drive, Belcamp, Maryland 21017 USA
Tel: +1 410 931 7500 or 800 533 3958, Fax: +1 410 931 7524,
Email: info@safenet-inc.com

EMEA Headquarters:
Tel: +44 (0) 1276 608 000, Email: info.emea@safenet-inc.com

APAC Headquarters:
Tel: + 852 3157 7111, Email: info.apac@safenet-inc.com

For all office locations and contact information, please visit
www.safenet-inc.com/company/contact.asp

©2009 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are
registered trademarks of SafeNet.
All other product names are trademarks of their respective owners.
PB-SafeXcel_IP-96.07.29.09