

Hardware Offload with QuickSec

Cryptographic Hardware Acceleration in Mobile Environments



SafeNet's solution to the increasing demand by mobile users for secure and responsive connectivity to corporate resources over Virtual Private Networks (VPNs) — accelerating cryptographic operations for superior computing performance.

True Mobile VPN Solutions

As mobile computing platforms mature and gain in processing power, network bandwidth, and usability features, they become viable platforms for the increasing demands of business applications. This is a welcome development for wireless carriers that focus on enterprise markets, as well as for enterprises that seek to enhance productivity by taking advantage of the mobility of their workforce.

In recent years, various semiconductor vendors who provide silicon for mobile devices have included security features that provide many advantages for cutting-edge security software. The CPUs contained in these mobile devices now provide these new, truly mobile VPNs with hardware-based cryptographic calculation of encryption and integrity protection algorithms.

Offload Crypto with QuickSec IPSec Toolkit

The cryptographic operations involved in the VPN software are computationally intensive. While this is rarely a problem for desktop computers, it poses several challenges on mobile devices that may often be required to operate on battery power and have limited CPU resources.

On mobile platforms, the offloading of cryptographic operations to hardware offers several important benefits:

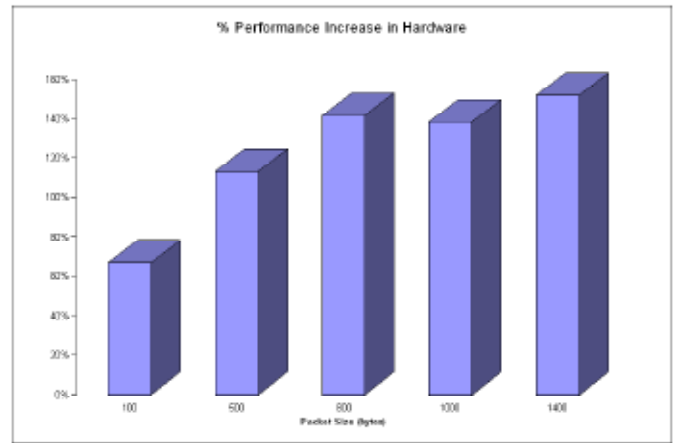
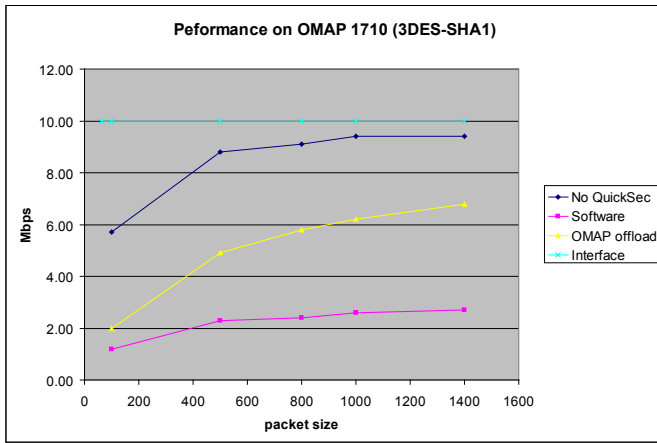
- Enhanced user experience – the CPU is available to serve the user instead of performing cryptographic calculations.
- Increased battery life – the power-hungry CPU is required to do less work.
- Increased throughput – a hardware-enabled VPN can provide over a 100% increase in processing speed over a software-based VPN.

QuickSec Client and Server

QuickSec is the most widely deployed carrier-grade IPSec security platform in the networking industry, delivering the advanced levels of protection, reliability, and performance mandated by OEM vendors and current industry standards. QuickSec is fully integrated with SafeNet's SafeXcel security processors to enable complete high-performance security systems

The QuickSec 4.1 Server and Client Toolkits are the first compatible client-side and server-side development tools, implementing the latest IPSec security features, including IKEv2, EAP authentication, MOBIKE, stateful TCP/IP firewall, IPv6/IPv4 support, 64-bit platform support, and, for hardware acceleration, pre-integration with high-speed security processors.





The figures above present the performance advantages that the use of dedicated cryptographic hardware acceleration provides on a mobile Texas Instruments OMAP 1710 processor. The offloading of the cryptographic calculations to specialized hardware cores on the OMAP processor the encrypted throughput of the mobile device can be doubled while relieving the general purpose processing core for other tasks.

SafeNet QuickSec— Reliability, Interoperability, and Quality

QuickSec’s support for the IPSec and IKE protocols provides a robust, scalable, and reliable solution that is the choice of dozens of telecom equipment vendors, VPN and firewall manufacturers, and other security-conscious hardware and software vendors. The IPSec and IKE implementations of the QuickSec Toolkit are mature, interoperable, and standards-compliant.

For use in mobile devices, SafeNet’s QuickSec technology has been optimized for:

- Attractive code and memory footprint – Mobile devices typically have serious constraints on memory and storage space.
- Deterministic and light runtime memory consumption – Allows the developer of mobile security software to ensure that the device will not become unresponsive due to the VPN software’s resource usage.
- Maximum efficiency – Battery powered devices need to run efficient software to ensure maximum battery life.

Benefits

There are significant benefits to using QuickSec Client and Server, for cryptographic hardware acceleration, including:

- Faster packet processing
- Lower power consumption
- Significant reduction in energy required to encrypt data
- CPU is free to perform other tasks
- Reduced heat
- Increased data throughput
- Increased battery life

About SafeNet Inc.

SafeNet’s award-winning security systems are deployed by leading global telecommunications, networking, and semiconductor vendors who trust SafeNet’s best-in-class security solutions for their next-generation networking products. SafeNet OEM customers include Nokia, Ericsson, NEC, AMCC, AMD, Azaire Networks, Cisco, Hitachi, HP, Juniper Networks, PMCSierra, Lucent Technologies, Nortel, Siemens, Samsung, and Texas Instruments. For more information about SafeNet’s embedded security systems, please visit <http://www.safenet-inc.com/OEM>



www.safenet-inc.com

Corporate: 4690 Millennium Drive □ Belcamp □ Maryland □ 21017 □ USA

Phone: +1 410.931.7500 or 800.533.3958

Email: OEMNetworking@safenet-inc.com

©2007 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners.