

QuickSec/IPsec Server Toolkit is a complete IPsec development toolkit that provides carrier-grade IPsec VPN solution for networking device developers. QuickSec/IPsec Server Toolkit enables robust and standards-compliant authentication, confidentiality, and data integrity for security gateways, routers and network servers. With hundreds of proven OEM implementations, QuickSec provides the advanced levels of protection, reliability, and performance mandated by OEM customers and industry standards.



## Benefits

**Carrier-grade IPsec Security Solution**

**Secure Mobility with Support for MOBIKE**

**Proven Reliability and Interoperability**

**Seamless & Massive Scalability with true multicore support**

**Standards-Based VPNC Certified Interoperability**

**Broad OS and Hardware Acceleration Support**

**Deterministic Memory Allocation and Resource Utilization**

**Integrated Client and Server-side IPsec Toolkits**

**Reduced Development Costs and Shortened Time to Market**

**World-wide Developer-level OEM Customer Support**

**Support for the Latest Industry Standards Resulting in Future-proof Security Implementations**

**Clean, Well Documented Source Code**

## Secure Mobility with MOBIKE

Fully interoperable with QuickSec and other standard-based clients, the server toolkit includes IKEv2 as well as MOBIKE for mobile VPN client support. MOBIKE is a mobility and multihoming addition to the IKEv2 key exchange protocol specified by IETF. It enables seamless roaming of IPsec VPN clients from one IP network to another without terminating and re-negotiating the secure VPN connection.

## Complete Security Solution

The QuickSec security toolkits provide a complete, standards-compliant, and interoperable Suite B IPsec protocol implementation including IPsec cryptography algorithms such as AES, DES, 3DES, RSA, SHA-1, SHA-2, MD5, Diffie-Hellman, ECC DH, ECC DSA, and PKI.

QuickSec/IPsec Server Toolkit features a broad range of platform support including, but not limited to; Linux 2.4 / 2.6, MontaVista Linux, VxWorks, and NetBSD. The ANSI C source code delivery of the toolkit facilitates the easy porting of the implementation to other platforms.

## Server and Client IPsec Toolkit

The QuickSec/IPsec Server and Client Toolkits form a compatible client- and server-side development tool solution that implements the most current IPsec security features including MOBIKE, IKEv2, stateful TCP/IP firewall, IPv6/IPv4 support, 64-bit platform support, and pre-integration with high-speed security processors for hardware acceleration.

## Advanced Features

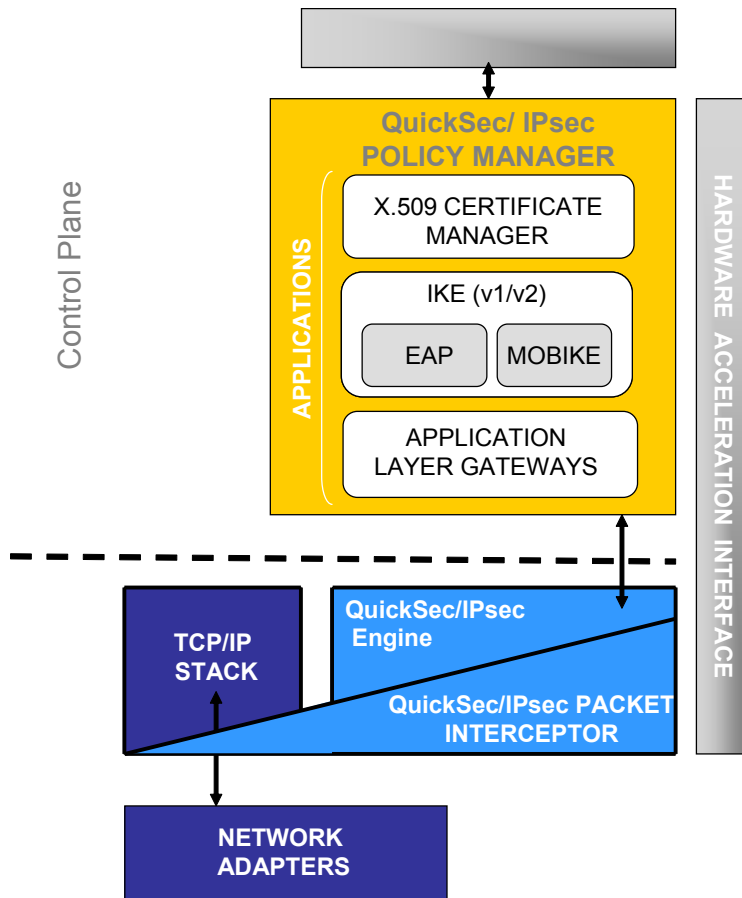
The server toolkit also includes remote access features and high availability APIs for import and export of IPsec security associations for device redundancy and failover. The small runtime footprint with linear deterministic memory allocation ensures seamless scalability to meet the highest performance demands. QuickSec also scales very well on multi-core architectures.

## Robust Security Performance through Hardware Acceleration

To accelerate performance-critical security algorithms and protocols, QuickSec supports many popular security processors in the market, including SafeNet's SafeXcel 51x0, 1141, 174x, and 184x series, and provides a well documented API for adding support to new or proprietary crypto hardware.

## Security SoC Platform Support

The QuickSec Toolkits are also an ideal IPsec solution for security-enabled SoCs from silicon vendors that have integrated SafeNet's hardware security engines into their products to provide robust, high-speed security functions. In addition to seamless integration with all third party SoCs, QuickSec has been optimized to interoperate with the SafeNet security engines embedded in devices from vendors such as AMCC, AMD, and PMC-Sierra, resulting in excellent security system performance and unparalleled ease of integration.



QuickSec/IPsec Server Toolkit - Architecture

## SafeNet Embedded Security Solutions

SafeNet is the only vendor that provides complete and proven IPsec and MACsec security solutions, including QuickSec IPsec and MACsec security toolkits, SafeXcel security processors, and silicon-proven semiconductor IP - delivering superior protection while reducing cost and time to market for networking OEMs.

SafeNet is the only supplier of complete security solutions that enable developers to integrate superior protection into networking products, while reducing cost and time to market.

SafeNet's award-winning security systems are deployed by leading global telecommunications, networking, and semiconductor vendors that trust SafeNet's best-in-class security solutions for their next-generation networking products.

SafeNet OEM customers include companies such as AMCC, AMD, Azaire Networks, Cisco, Hitachi, HP, Juniper Networks, PMC-Sierra, Alcatel-Lucent Technologies, NEC, Nortel, Siemens, Samsung, and Texas Instruments.

For more information about SafeNet's embedded security systems, please [http://www.safenet-inc.com/products/swTK/QuickSec\\_5\\_Server\\_Toolkit.asp](http://www.safenet-inc.com/products/swTK/QuickSec_5_Server_Toolkit.asp).

## Technical Specifications

### Complete IPsec Cryptography

- AES, DES, 3DES, RSA, SHA-1, SHA-2, MD5, Diffie-Hellman, ECC DH, ECC DSA and PKI

### IKE Policy Manager

- Dual-mode IKEv2/IKEv1 policy manager with auto-negotiation and IKEv1 fallback features

### Authentication

- MOBIKE
- Robust IKEv2/v1 authentication
- Multiple authentication support
- X.509 certificates
- XAUTH
- EAP
- Pre-shared keys
- Dead peer detection
- Re-keying

### Remote Access Support

- Built-in IP address allocation
- NAT, NAT Traversal
- EAP authentication
  - EAP-SIM
  - EAP-AKA
  - EAP-MD5
  - EAP-TLS
- RADIUS server authentication

### Other Features

- IPv4 and IPv6 support
- High availability APIs import/export of IPsec SAs
- Stateful TCP/IP firewall with attack prevention
- ALG framework with example implementations for common protocols (HTTP, SIP, FTP, CIFS)
- IPCOMP with the deflate algorithm
- Support for OCF (Open Cryptographic Framework)
- Support for Linux 4K kernel stacks

### Platform Support

- Linux 2.6
- MontaVista Linux
- VxWorks
- Microsoft Windows XP (32-bit and 64-bit)
- Microsoft Windows Vista (32-bit and 64-bit)
- Microsoft Windows Server 2003 (32-bit and 64-bit)
- Microsoft Windows Server 2008 and 2008 R2

### Hardware Acceleration

- SafeXcel-51x0, SafeXcel-174x, and SafeXcel-124x
- AMCC 440 EPx/GRx
- PMC-Sierra MSP 8520
- Various 3rd party crypto processors
- Cavium Octeon



[www.safenet-inc.com](http://www.safenet-inc.com)

#### 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](mailto:info@safenet-inc.com)

#### EMEA Headquarters:

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

#### APAC Headquarters:

Tel: + 852 3157 7111, Email: [info.apac@safenet-inc.com](mailto:info.apac@safenet-inc.com)

For all office locations and contact information, please visit [www.safenet-inc.com/company/contact.asp](http://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-QuickSecIPSec 08.27.09