QuickSec Client Toolkit enables developers to build robust IPsec client functionality into mobile and remote networking devices. QuickSec is the first small-footprint security toolkit in the market to support the latest mobile VPN standards and platforms, including the mobility and multi-homing protocol MOBIKE, as well as mobile platforms such as Windows Mobile.

**Secure Mobility with MOBIKE**

Fully interoperable with QuickSec/IPsec and other IPsec standard-based gateways, the client toolkit includes IKEv2/v1 as well as MOBIKE for mobile IPsec support. MOBIKE is a mobility and multi-homing extension to the IKEv2 key exchange protocol specified by the IETF. It enables seamless roaming of IPsec clients from one IP network to another without terminating and re-negotiating the secure connection.

**Server and Client IPsec Toolkit**

The QuickSec Server and Client Toolkits are the compatible client- and server-side development tools that implement the most current IPsec security features including IKEv2, MOBIKE, a stateful TCP/IP firewall, IPv6/IPv4 support, 64-bit platform support, and pre-integration with specialized mobile processors providing cryptographic hardware offload.

**Complete Security Solution**

The QuickSec Client Toolkit provides a complete, standards compliant, and interoperable IPsec protocol implementation including cryptographic algorithms such as AES, 3DES, SHA-1, SHA-2, MD5, Diffie-Hellman, RSA, DSA, as well as facilities for accelerating the cryptographic operations with specialized hardware (available, for example, for TI OMAP mobile application processors). The client toolkit provides platform adaptation code for such popular platforms as Windows Vista and XP, Windows Mobile 5 and 6, and MontaVista Mobilinux. The ANSI C source code delivery of the toolkit facilitates the easy porting of the implementation to other platforms.

**IKEv2 with SIM-based authentication (EAP-SIM/AKA)**

QuickSec Client Toolkit's dual-mode IKE policy manager allows devices to auto-negotiate an IKEv2 connection or automatically fall back to IKEv1 if IKEv2 is not supported by the communicating peer. This feature ensures seamless interoperability with the large base of legacy VPN hardware and software.

QuickSec's IKE implementation includes an EAP framework for extending IKE authentication to utilize SIM and USIM UICCs deployed in mobile networks. QuickSec also comes with multiple authentication support for IKEv2 QuickSec is widely deployed in various IMS GWs, which guarantees clients' interoperability in these use cases.

**Small Footprint**

QuickSec Client Toolkit provides an intelligent architecture that enables minimum runtime memory allocation thereby freeing CPU and memory resources to other tasks. This ensures seamless scalability to meet the highest performance demands.

To further minimize footprint, system designers can easily leave out client toolkit features that are not used by the client application.

SafeNet is the only vendor that provides complete and proven security systems, including QuickSec security toolkits, SafeXcel security processors, and silicon-proven semiconductor IP – delivering superior protection while reducing cost and time to market for networking OEMs.
**SafeNet Embedded Security Solutions**

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.


---

**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**
- Robust IKEv2/v1 implementation
- Multiple authentication support
- MOBIKE
- X.509 certificates
- XAUTH
- EAP
  - EAP-SIM
  - EAP-AKA
  - EAP-MD5
  - EAP-TLS
- Pre-shared keys
- Dead peer detection
- Re-keying

**Remote Access Support**
- Built-in remote access client
- Virtual IP interface
- IKE Configuration mode/payload
- NAT, NAT Traversal
- RADIUS server authentication

**Other Features**
- Multi-layer stateful TCP/IP firewall with attack prevention
- IPv4 / IPv6 support

**Platform Support**
- Linux 2.6
- MontaVista Linux
- Microsoft Windows XP, Windows Vista and Windows 7 (32-bit and 64-bit)
- Microsoft Windows Server 2008
- VxWorks
- Windows Mobile 5.x and 6.x