EMBEDDED
SECURITY SOLUTIONS

QuickSec®/IPsec
Server Toolkit

Benefits

- Carrier-grade IPsec Security Solution
- Secures Mobility with MOBIKE
- Proven Reliability and Interoperability
- Seamless & Massive Scalability with true multicore support
- Standards Bassed 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
- Worldwide Developer-level OEM Customer Support
- Support for the Latest Industry Standards Resulting in Futureproof Security Implementations
- Clean, Well Documented Source Code

QuickSec®/IPsec Server Toolkit enables developers to build robust IPsec gateway functionality quickly and costefficiently. QuickSec® is an IPsec toolkit written in highly portable C source code and delivered with extensive documentation. It support all IPsec RFCs and is designed and tested for high interoperability. It is widely deployed on platforms including Linux, VxWorks and NetBSD and in products such as enterprise security gateways, high security government appliances, high capacity carriers' gateways, printers..,

Accelerate time-to-market and reduce R&D costs

IPsec is a complex protocol with many options and features. Inside Secure team has a long experience in delivering IPsec technology to leading gateway vendors and supporting IPsec integration in a wide variety of platforms. By using QuickSec®/IPsec Server Toolkit, you benefit from a proven, tested product that is updated and maintained regularly. You also benefit from a support organisation manned by experienced engineers that can guide you to integrate in your specific environment.

Complete IPsec implementation

The QuickSec®/IPsec Server toolkit is a well documented and portable ANSI C source code implementation of IPsec. This complete, standards-compliant implementation supports over 80 RFCs. The interoperability is verified in INSIDE Secure interoperability laboratory and proven by hundreds of commercial products. Extensive cryptographic libraries provides full support for suite B and a wide set of algorithms such as AES, DES, 3DES, RSA, SHA-1, SHA-2, MD5, Diffie-Hellman, EC DH, EC DSA, and PKI. QuickSec®/IPsec Server Toolkit is used on a broad range of platforms including, but not limited to, Linux, MontaVista Linux, VxWorks, and NetBSD.

Designed for high performance

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 well on multi-core architectures.

Robust Security Performance through Hardware Acceleration

To accelerate performance-critical security algorithms and protocols, QuickSec®/IPsec is commonly deployed with security processors such as Cavium Octeon or Nitrox. It also provides support for Tilera Gx series. Its well documented APIs simplify the integration with a wide range of crypto hardwares, including plain crypto cores, packet engines, inline hardware accelerators, bare-metal fastpaths as well as public key accelerators. It is also an ideal IPsec solution for security-enabled SoCs from silicon vendors that have integrated INSIDE Secure's SafeXcel® Embedded Security IP Packet Engine into their products to provide robust, high-speed security functions.

driving trust™

www.insidesecure.com

True Multicore Architecture

QuickSec®/IPsec Server offers true multicore support for maxium scalability. The QuickSec® data plane supports multicore bare-metal implementations as well as various harware accelerated and software based architectures. The QuickSec® Policy Manager and IKE stacks can utilize multicore environments to achieve best tunnel setup rates optionally taking advantage of hardware acceleration.

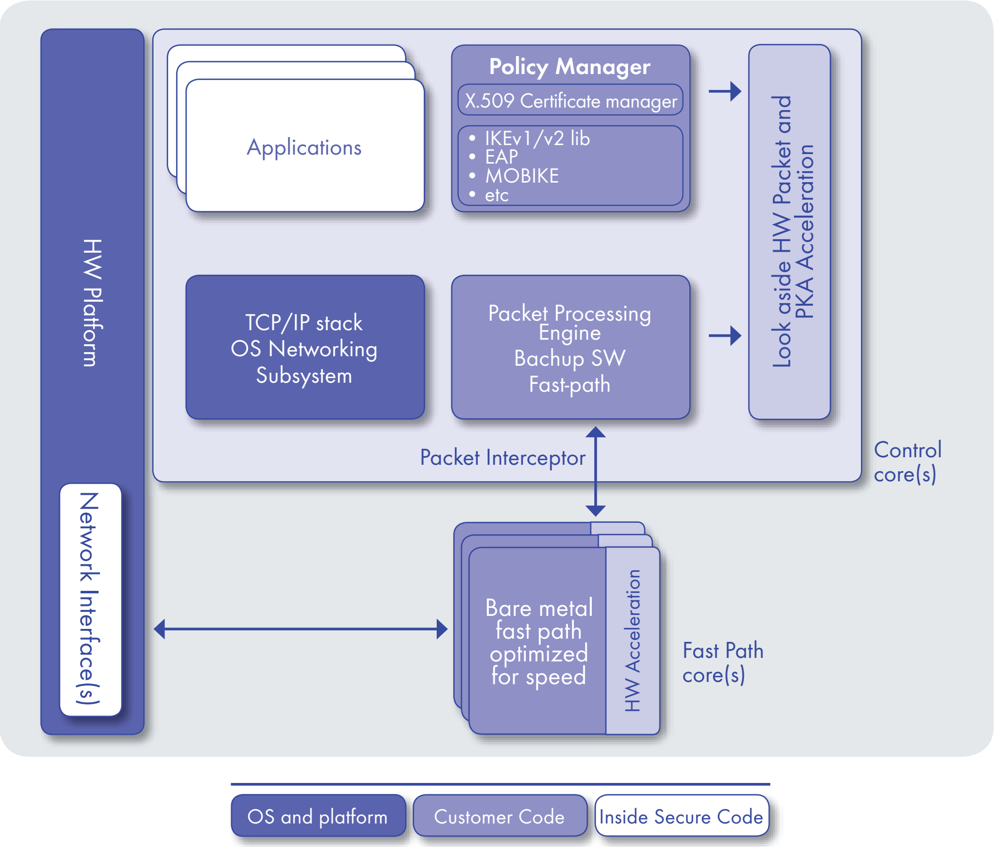
INSIDE Secure Extensive Security Solutions

INSIDE Secure is the only vendor that provides complete and proven Layer 2, 3 and 4 security toolkits, including not only QuickSec® IPsec server and client but also MACsec and MatrixSSL toolkits. INSIDE Secure's semiconductor security IP is designed in by many SoC to accelerate packet processing and drastically reduce energy consumption. They are ideal solution to integrate with INSIDE Secure toolkit products.
In addition, INSIDE Secure provides a broad range of solutions to protect content and data including DRM, HDCP, DTCP, DAR, FIPS validated crypto, Secure Elements, payment solutions, secure platform solutions.

With decades of security innovation and expertise, INSIDE Secure has become the leader in complete solutions for embedded security applications. Our hardware, firmware, middleware, software, and intellectual property work together, enabling customers to secure everything from mobile devices and transactions to payment, access, and the Internet of Things. Our security expertise and innovation provide 360-degree coverage of customers' security challenges, enabling us to bring the right level of security to the right challenge and add value to customers' solutions.

INSIDE Secure's award-winning security products are deployed by leading global telecommunications, networking and semiconductor vendors and innovative startups that trust INSIDE's best-inclass security solutions for their next-generation networking products.

INSIDE Secure is the ideal partner to integrate superior protection into networking products, while reducing cost and time to market for networking OEMs.



→ Supports all major VPN use cases:

- IKEv1 and IKEv2
- MOBIKE (mobility extension of IKEv2)
- ESH and AH, tunnel and transport modes
- NAT-T, Dead Peer Detection, L2TP over IPsec support, IPcomp...
- Stateful firewall for protection against network level attacks
- Crypto library compliant with Suite B and FIPS 140-2 Level 1 Requirements
- NIST Special Publication 800-131A conformance

→ All common authentication mechanisms

- Shared secret, XAUTH, RADIUS, EAP
- X509v3 certificates with CRL and OCSP

→ Full IPv4 and IPv6 support

- IPv6 over IPv6, IPv6 over IPv4 and vice versa
- IPv4 and IPv6 address allocation (e.g. with DHCP)

Information in this document is not intended to be legally binding. INSIDE Secure products are sold subject to INSIDE Secure Terms & Conditions of Sale or the provisions of any agreements entered into and executed by INSIDE Secure and the customer. INSIDE Secure,® Inside Secure logo and combinations thereof, and others are registered ® trademarks or tradenames of INSIDE Secure or its subsidiaries. Other terms and product names may be trademarks of others. The products described herein may be protected by one or more of the patents and/or patent applications listed in related datasheets, such document being available on request under specific conditions. Additional patents or patent applications may also apply depending on geographic regions.

For further details on all of INSIDE's security solutions, visit www.insidesecure.com

0214 - Document non contractuel - zaostratecrea.com