inside SECURE Secure Communications and Protocols

QUICKSEC® IPSEC TOOLKIT

Client/Server software for Clouds and embedded deployments

• Benefits

- Accelerate time to market with proven security
- Reduce risks with professional security
- Professional support
- Regular updates by cryptographic experts
- No GPL constraint
- Proven Reliability and Interoperability
- Seamless & Massive Scalability
- Deployed with a million concurrent tunnels
- 2000 tunnel setup rates on only 2 cores
- Multicore capable control plane
- Deterministic Memory Allocation
- Integrated Client and Server IPsec Toolkits
- FIPS140-2 certified crypto available

FIPS VALIDATED 140-2

FIPS Inside: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments

Highlights

QuickSec® Toolkit is a complete software stack to build robust IPsec VPN gateway or IPsec Client. QuickSec® Toolkit is a IPsec SDK written in highly portable C source code and free of GPL constraints. It enables robust and standards compliant authentication, confidentiality and data integrity. It is widely used in products such as enterprise security gateways, high security government appliances, high capacity carriers' gateways, SD-WAN, eNodeB, mobile devices and printers. It is deployed on platforms including Linux, Windows as well as in Cloud (SDN/NFV) environment. It is available as a client toolkit, a server toolkit or as a bundle.

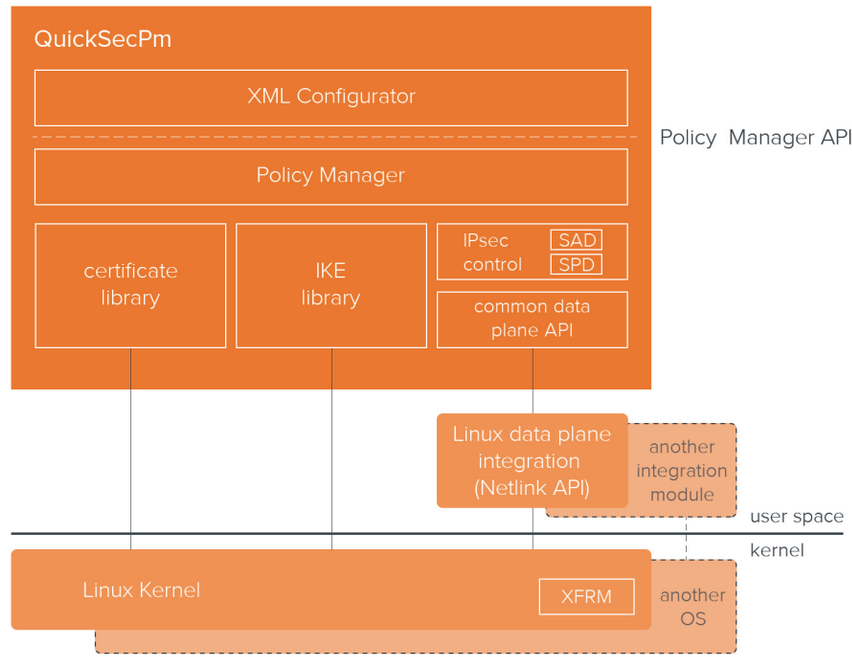
Accelerate time-to-market and reduce R&D costs

IPsec is a complex protocol with many options and features. The QuickSec 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 Toolkit, you benefit from a proven, tested product that is updated and maintained regularly by our security experts. You also benefit from a support organization manned by experienced engineers that can guide you throughout the life time of your product.

Designed to integrate with any dataplane

Most platform vendors provide an IPsec dataplane optimized for their platform. It is therefore essential that QuickSec Toolkit integrates seamlessly with any IPsec dataplane.

It is pre-integrated with Netlink API. It seamlessly integrates with Linux kernel IPsec dataplane for embedded integration, or with 6WINDGate's IPsec dataplane for Cloud's integration (with DPDK). It is also designed to integrate with any IPsec dataplane through its Common Dataplane API.



Interoperability

As our customers develop products that must work seamlessly with various IPsec implementations, QuickSec® Toolkit supports the 90+ standard specifications required to work with the various flavor of IPsec. The QuickSec team has worked on IPsec technology for 20 years, and INSIDE Secure co-authored the latest IKEv2 specification (RFC 7296). Interoperability is verified as part of the QA process in INSIDE Secure's own laboratory.

High scalability

QuickSec® Server Toolkit is designed for high scalability. It has been deployed with over 1 million IPsec tunnels. Large deployments require:

• High session set-up rate: QuickSec is able to reach 2000 IPsec tunnel establishment per second with only 2 CPU cores. It also scales well on multicore architecture and performances are stable with high number of sessions. It can leverage any cryptographic hardware acceleration present on the platform.

• High Availability (HA): The server toolkit includes high availability APIs for import and export of IKE and IPsec SAs (Security Association) for device redundancy and failover.

• Gradual restart: When a gateway with a large number of IPsec connections restarts, re-establishing all connections may be time consuming. Instead it is possible to only restart the IPsec connections when needed by triggering the IKE session establishment only when packets are received.

• Easy debugging: To resolve problems in large deployments without impacting performance, it allows to request detailed logs only for specific tunnels.

Multi-tenancy

To allow a Cloud network to provide multiple networks or an eNodeB to support multiple operators, QuickSec Toolkit supports multiple VRF (Virtual Routing and Forwarding) instance.

Technical Specifications

IKE (Internet Key Exchange)

• IKEv2 (RFC 7296)
• IKEv2 Fragmentation (RFC 7383)
• IKEv2 Redirect (RFC 5685)
• MOBIKE (RFC 4555, RFC 4621)
• IKEv1 main mode and aggressive mode
• Perfect Forward Secrecy (PFS) option
• Re-keying, Dead Peer Detection (DPD), NAT-Traversal (NAT-T)
• Authentication: Pre-Shared Keys (PSK), XAUTH, Certificates ((full PKI support), Extensible Authentication Protocol (EAP-SIM, EAP-AKA, EAP-MD5, EAP-TLS), RADIUS, Multiple Authentication (RFC 4739)
• IPv4 and IPv6 support: including DHCPv4 and DHCPv6
• RSA, DSA and ECDSA public key algorithms (IKE signature modes only)
• RSA signature support for SHA2 in IKE according to NIST Special Publication 800-131A
• Remote Access Support: Virtual adapter configured by the server
• Built-in IP address allocation

Certificates and PKI Functionality

• X.509v3 (PKIX) certificate profile and certificate revocation list (CRL) support
• Certificate distribution point support, with LDAP and HTTP
• On-line certificate status checking, using OCSP
• Standard-based certificate enrollment support, using SCEP and CMP.
• RSA signature for SHA2 in certificates according to NIST Special Publication 800-131A

Complete IPsec Cryptography

• Cipher Algorithms : AES, AES-CCM, AES-GCM, AES-GCM-64, GMAC-AES, 3DES
• MAC Algorithms : SHA-1, SHA-2, MD5, GMAC-AES, AES-XCBC
• Asymmetric cryptography algorithms : RSA, Diffie-Hellman, ECC DH, ECC DSA
• PKCS#1, PKCS#5, PKCS#7, PKCS#8, PKCS#10, PKCS#12
• Elliptic Curve Cryptography : Brainpool Elliptic Curves (RFC 5639, RFC 6932), ECDSA (RFC 4754)ECP Groups (RFC 5903), Elliptic Curve Digital Signature (ECDS)

Platform Support

• Linux : QuickSec client and server Toolkits supports all Linux versions
• Windows 7, 8, 10 : QuickSec Client Toolkit only
• Other OS's through portability layer

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

inside SECURE
Driving Trust