

Treck IPsec/IKE

product information

High Performance Embedded systems are the key technologies fueling innovative, high-growth applications of today's fast-growing markets. These include digital wireless, broadband access, digital audio, high-resolution imaging and digital motor control. A key reason for embedding pre-designed functions is to reduce the time it takes to get complex systems to market while speeding their proliferation.

The ability to rapidly design, test, debug and manufacture a device is crucial to the continued success of the electronics industry.

Next Header	Payload Length	Reserved
Security Parameter Index (SPI)		
Sequence Number		
Authentication Data (For IPsec, this field is 96 bits)		

The embedded systems market is integrating security and computing systems capable of adapting to a range of specific applications. If you are designing security platforms, you need a top of the line networking stack to reduce your capital expenditure risk and meet the stringent requirements of the market.

Treck's networking protocols are specifically designed for embedded systems. We have created fast, efficient and reliable plug and play communication protocols so you can concentrate on your core competency and build designs that meet your "time to market" needs. Treck's IPsec is an ideal security protocol for embedded systems designers.

IPsec/IKE protocols address security needs that range from portable wireless devices to routers. Written specifically for embedded systems, Treck IPsec is tightly integrated with our Treck IPv4/IPv6 product for optimal performance.

Treck IPsec/IKE ensures that data transmitted across an unsecured network such as the Internet, can be free of observation, spoofing, or modification of any kind. There are no artificial limits on the number of connections; expandability is only restricted by available resources.

True Zero Copy

Treck products are zero copy from the application all the way through the driver, including TCP, this increases processing speed.

Written specifically for embedded systems

Treck IPsec is not a Bump in the Stack implementation of IPsec. It is tightly integrated with our *Treck TCP/IPv6* product for optimal performance.

Security Parameter Index (SPI)		
Sequence Number		
Initial Vector		
Payload Data		
Padding	Pad Length	Next Header
Authentication Data (For IPsec, this field is 96 bits)		



Mobile



Network

Treck IPsec/IKE

product features

Product Features

- Lifetime of SAs using volume (kilobytes)
- Lifetime of SAs using time (seconds)
- X.509 digital certificates and RSA/DSA digital signatures
- Tunnel and transport modes
- Nested tunnels
- SA bundles (ESP used with AH)
- Policy Management API, with bulk-load capability
- Policy and SA lookup using standard selectors, including:
 - local or remote IP address, subnet address or address range
 - local port number
 - remote port number
 - protocol ID
- AH transforms MD5 and SHA-1
- ESP transforms DES, 3DES, RC5, CAST, BLOWFISH, AES (RIJNDAEL), TWOFISH
- IKE phase 1 Main Mode, Aggressive Mode, IKE phase 2 Quick Mode
- IKE perfect forward secrecy using predefined groups
- IKE encryption using DES, 3DES, BLOWFISH, RC5-R16-B64, CAST, AES (RIJNDAEL) and TWOFISH
- IKE hash algorithms MD5 and SHA-1
- IKE authentication using pre-shared keys
- ISAKMP Informational Exchanges: DELETE, INITIAL-CONTACT, error notification
- RIPEMD-160-96 hash algorithm
- Optimized specifically for embedded systems
- Diffie-Hellman groups 1, 2 and 5

RFCs Supported

2401 Security Architecture for IP

2411 IP Security Document Roadmap

Basic protocols

2402 IP Authentication Header

2406 IP Encapsulating Security Payload (ESP)

Key management

2407 The Internet IP Security Domain of Interpretation for ISAKMP

2408 Internet Security Association and Key Management Protocol (ISAKMP)

2409 The Internet Key Exchange (IKE)

2412 The OAKLEY Key Determination Protocol

2437 PKCS #1 RSA Cryptography Specification v2

2459 Internet x509 Public Key Infrastructure Certificate and CRL

Details of various items used

2085 HMAC-MD5 IP Authentication with Replay Prevention

2104 HMAC: Keyed-Hashing for Message Authentication

2202 Test Cases for HMAC-MD5 and HMAC-SHA-1

2403 The Use of HMAC-MD5-96 within ESP and AH

2404 The Use of HMAC-SHA-1-96 within ESP and AH

2405 The ESP DES-CBC Cipher Algorithm with Explicit IV

2410 The NULL Encryption Algorithm and its use with IPsec

2451 The ESP CBC-Mode Cipher Algorithms

2144 The CAST-128 Encryption Algorithm

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)

For more information, please visit www.treck.com.



Mobile



Network

Treck Inc.