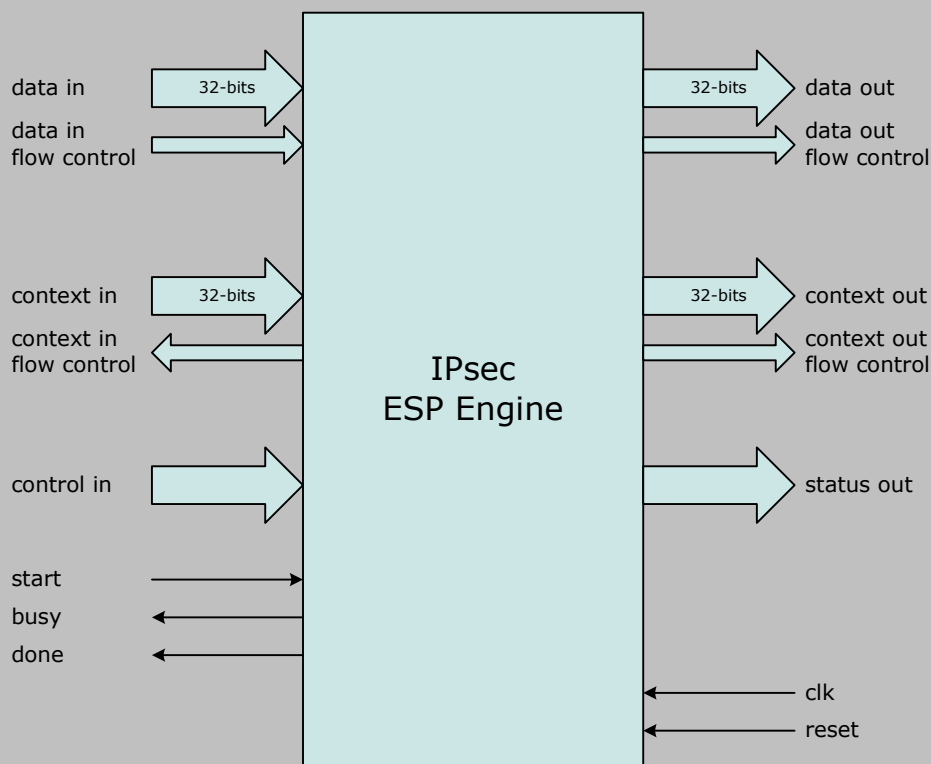


# Helion Technology

## DATASHEET - IPsec ESP Engine for Xilinx FPGA



### Features

- Designed for hardware acceleration of IPsec ESP protocol
- Supports all mandatory and proposed IPsec ESP confidentiality and authentication algorithms
- Suitable for use in IPv4 and IPv6 IPsec Transport and Tunnel mode applications
- Extended (64-bit) Sequence Number support for IKEv2
- Supports all proposed ESP security service combinations
- Supports insertion of padding for Traffic Flow Confidentiality (TFC)
- Automatic ESP padding generation and checking
- Supports Gigabit/sec throughputs

### Deliverables

- Target specific netlist or fully synthesisable RTL VHDL
- Verilog/VHDL simulation model and testbench
- User documentation

## Overview

Built on the success of Helion's industry proven cryptographic IP cores, the Helion ESP Engine provides hardware acceleration of the key computationally intensive algorithms required by the IPsec Encapsulating Security Payload (ESP) protocol. Its modular architecture provides the flexibility to support only those cryptographic algorithms required for a particular IPsec application to yield an optimum logic area and performance trade-off.

The ESP Engine is suitable for use in both IPv4 and IPv6 IPsec applications, and can support both Transport and Tunnel mode operation. It supports all mandatory ESP algorithms as defined in RFC4835 including 3DES-CBC, AES-CBC, AES-CTR, HMAC-SHA-1-96, and AES-XCBC-MAC-96, as well as the proposed combined mode algorithms such as AES-CCM and AES-GCM. In addition to cryptographic acceleration, the ESP Engine also performs padding generation and checking in accordance with RFC4303, and fully supports Traffic Flow Confidentiality padding generation.

## Helion Technology Limited

Ash House, Breckenwood Road,  
Fulbourn, Cambridge CB21 5DQ, England



# Functional Description

The Helion ESP Engine is designed to interface easily into a system datapath utilising external packet data FIFOs in a typical IPsec application. Data flow is controlled automatically by the ESP Engine using the number of data words available in the input FIFO, and the amount of free space in the output FIFO. A separate memory mapped context interface provides a means for the ESP Engine to access the Security Association information which must be provided by the external host that implements the IPsec Security Policy. The Security Association context includes all information required to provide ESP confidentiality and authentication services for the packet; cryptographic keys and IVs, ESP packet header SPI and Sequence Number fields etc.

Once the context has been setup by the host, the ESP Engine may be started. At this point a number of per packet control inputs (including ESP security service type, packet length and direction) are sampled and loading of the context will commence as the Engine pre-processes Keys and IVs for the cryptographic algorithms. Once pre-processing is complete, the Engine will encrypt/decrypt the input packet as it arrives at its input interface before forwarding the resulting packet to the output interface.

External control of the ESP Engine uses a simple start, busy and done interface with status outputs. The status outputs are guaranteed valid on assertion of done and indicate the success or otherwise of the ESP packet processing including padding checking, ICV integrity checking, and the output packet length in bytes.

## Logic Utilisation and Performance

The Helion ESP Engine makes extensive use of Xilinx-specific architectural features in order to achieve high performance combined with extremely efficient logic resource utilisation. It can be configured at time of order to offer any combination of the supported confidentiality and authentication algorithms. Various performance options are also available which allow throughput and area to be matched to a user's requirements. For a given clock frequency, the maximum ESP Engine data throughput is dependent on the IPsec security service selected, the input packet length, and the throughput of the selected cryptographic modules.

The tables below show logic area and performance figures for a typical ESP Engine configuration implementing the mandatory **AES-CBC** and **3DES-CBC** confidentiality algorithms and **HMAC-SHA-1-96** authentication algorithm in different Xilinx FPGA families. The maximum data throughput figures shown are for AES-CBC confidentiality and HMAC-SHA-1-96 authentication using a 1500 byte packet length. The first table shows an ESP engine with high rate AES and the second table with the lower rate AES option, offering a lower area alternative. Figures for other algorithms, packet lengths or device speed grades are available from Helion on request.

	—ESP with high rate AES option—			—ESP with lower rate AES option—		
technology	Spartan3 -5	Virtex4 -11	Virtex5 -3	Spartan3 -5	Virtex4 -11	Virtex5 -3
logic resource	3802 slices 18 RAMB16	3796 slices 18 RAMB16	2342 slices No RAM	2618 slices 5 RAMB16	2626 slices 5 RAMB16	1615 slices No RAM
max clock	100 MHz	191 MHz	243 MHz	111 MHz	190 MHz	237 MHz
max throughput (AES+SHA-1)	473 Mbps	903 Mbps	1150 Mbps	258 Mbps	443 Mbps	552 Mbps

## More Information

For more detailed information on this or any of our other products and services, please contact Helion and we will be pleased to discuss how we can assist with your individual requirements.



### Helion Technology Limited

Ash House, Breckenwood Road,  
Fulbourn, Cambridge CB21 5DQ, England

tel: +44 (0)1223 500 924 email: [info@heliontech.com](mailto:info@heliontech.com)  
fax: +44 (0)1223 500 923 web: [www.heliontech.com](http://www.heliontech.com)