

The ESM-01 is the first in a family of Embedded Security Modules which are targeted at off the shelf security functions such as DTCP (the Digital Transmission Content Protection) rights management technology. This core complies with the standard specified by the DTLA (the DTCP Licensing Authority). DTCP was designed to protect high value digital content such as music and video for transmission over Firewire, USB, MOST (an automotive bus) and TCP/IP networks. This product brief outlines the ESM-01 to the extent that is possible under the confidentiality restriction agreed under the license between the DTLA and Elliptic. Detailed technical specifications for the ESM-01 can only be released to other DTCP licensees.

Key Features:

- AES and M6 symmetric encryption blocks
- SHA-1 Hashing
- Context cache to support of session interleaving
- Private Context with Non Volatile Memory Options
- AMBA/AHB interface available
- Hardware assist for DTCP compliant random number generation
- Low level API in C source code
- Companion DTCP Evaluation Software to be released Q2 2006

Applications:

- Consumer Electronics such as Cameras, DVD Players, Set-top Boxes, Media Gateways
- Automotive Applications in Entertainment Consoles

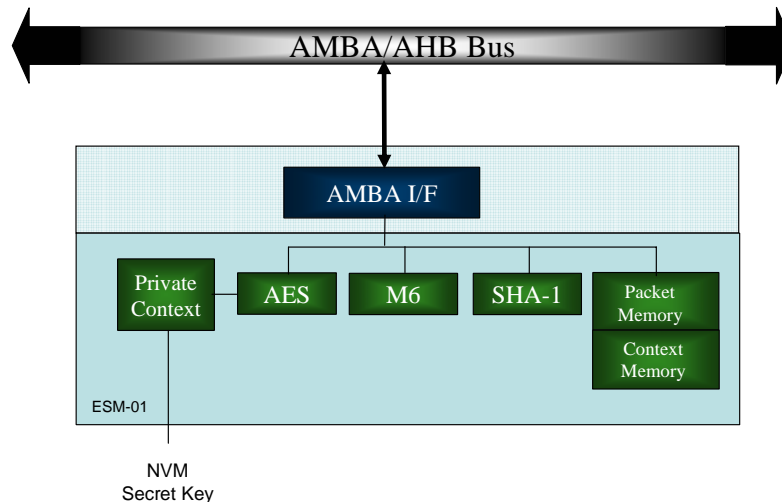


Figure 1 ESM-01 Block Diagram

Pin Description

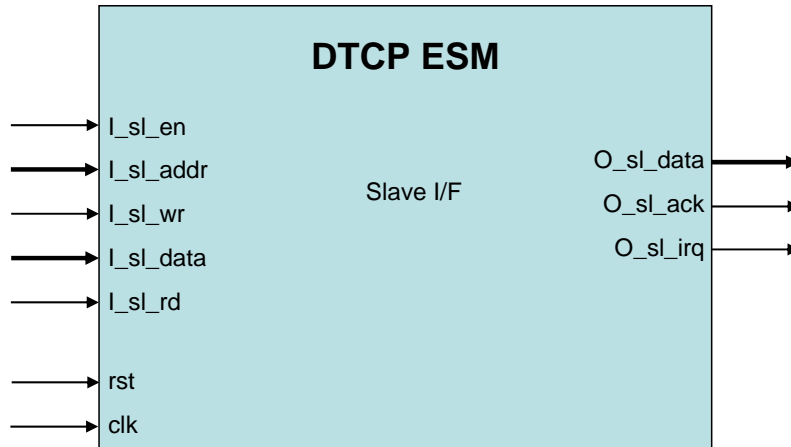


Figure 2 ESM-01 PinOut

The following table provides pin details including bit widths and descriptions.

| Signal Name | Bit Width | Direction | Description |
|---------------------------------------|-----------------|-----------|--|
| <i>System Pins</i> | | | |
| clk | 1 | input | System clock. All inputs are sampled on the rising edge of the clock. |
| rst | 1 | input | Asynchronous reset. Internal state returns to default value upon assertion (active high). |
| <i>Slave Interface from Processor</i> | | | |
| I_sl_en | 1 | input | Enable pin for the slave interface. All other inputs are ignored unless this pin is asserted. |
| I_sl_addr | 13 ¹ | input | Slave address to perform a read or write. This bus must be valid any time I_sl_wr or I_sl_rd (qualified with I_sl_en) is asserted. |

| Signal Name | Bit Width | Direction | Description |
|-------------|-----------|-----------|--|
| I_sl_wr | 1 | input | Write enable signal to write I_sl_data at address I_sl_addr . |
| I_sl_data | 32 | input | Data to write. This bus must be valid any time I_sl_wr (qualified with I_sl_en) is asserted. |
| I_sl_rd | 1 | input | Read enable signal to read data O_sl_data from address I_sl_addr. |
| O_sl_data | 32 | output | Output data bus; results of a read operation. |
| O_sl_ack | 1 | output | Acknowledge signal sent to processor. |
| O_sl_irq | 1 | output | Interrupt signal from engine. |

1. I_sl_addr bus is configurable depending on ESM packet buffer memory configuration.

Table 1 ESM-01 I/O

General Description

The DTLA was founded by Hitachi, Ltd., Intel Corporation, Sony Corporation, Toshiba Corporation and Matsushita Electric Industrial Co. Ltd. to build an interoperable, industry standard digital rights management design that could be used by manufacturers of consumer electronics products. The standard specifies the encryption of high value content, key exchange mechanisms, mutual authentication and repudiation of devices that have been compromised. Initially the DRM capabilities focused on high speed interconnection technologies such as Firewire and USB but they have been extended to include MOST for automotive applications and TCP/IP for broader deployment in home networks based on Ethernet and/or Wi-Fi. The licensing of the technology is governed by a Licensing Authority based in the United States called the Digital Transmission Licensing Authority - the web site for the DTLA can be found at:

www.dtcp.com

The license that Elliptic signed with the DTLA prohibits disclosure of the technical details of the rights management design except those aspects already in the public domain on the DTLA web site. Complete disclosure of the technical details for the ESM-01 are therefore only available to companies that have signed a license with the DTLA.

The ESM-01 consists of the DTCP ciphers – an AES cipher and a M6 cipher, a SHA-1 hashing block and secret key infrastructure that can be built around different non-volatile memory solutions such as fuses or embedded Flash memory such as Virage Logic NOVeA™. The secret key cannot be accessed outside the ESM and can be used to encrypt and decrypt DTLA secret values for storage in external memory without concern that the values might be visible to hackers. The core supports the encryption and decryption of content such as music and video and provides hardware assist for random number generation and authentication operations are required to meet the overall specification.

Performance and Gate Count

The ESM-01 is designed for applications in consumer electronic and automotive use. The current performance for symmetric encryption is specified in Table 2 below when the core is clocked at 100 MHz.

| Core | Throughput |
|-------|------------|
| AES | 200 Mbps |
| M6 | 300 Mbps |
| SHA-1 | 600 Mbps |

Table 2 ESM-01 Throughput Capabilities

Elliptic synthesis and simulation results indicate that the core could be clocked up to 167 MHz thereby doubling the throughput capability by using a high speed 0.13 micron process such as TSMC LV or UMC HS combined with a high performance libraries and memory.

At 100 MHz, the core synthesizes out to 60K ASIC gates. With the DTLA specified number of contexts and appropriately sized packet memory, the internal memory occupies 4 Kbytes of dual port memory. This is a factory configuration option that can be changed to accommodate higher performance applications.

Deliverables

The ESM-01 is available in soft IP form, either as a Netlist or HDL Source. The deliverables available are:

Netlist Licenses:

- Post synthesis netlist
- Testbench
- Simulation script
- Documentation

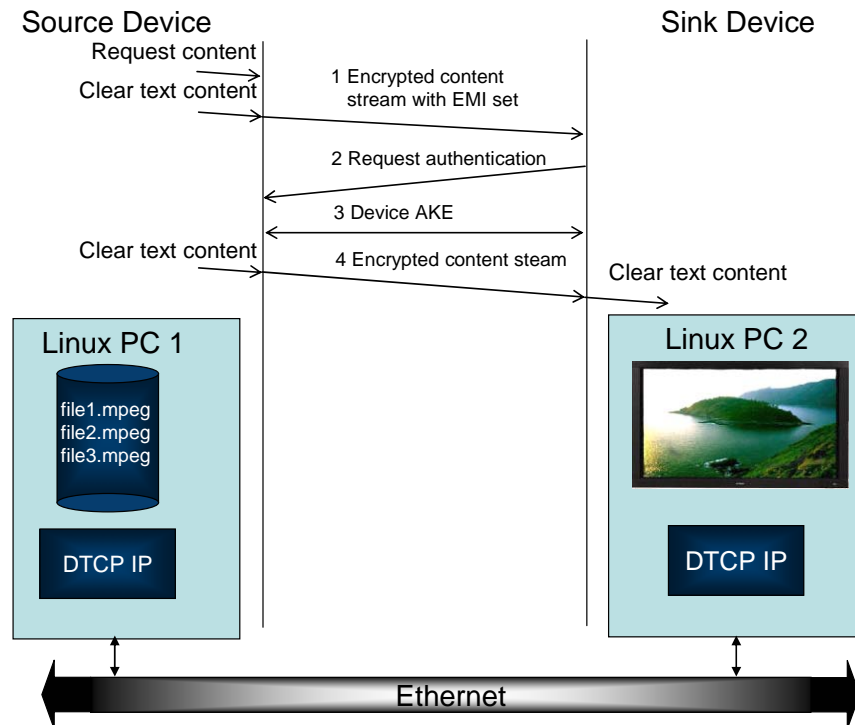
HDL Source Licenses:

- HDL
- Testbench
- Synthesis script
- Documentation

An FPGA load can be made available under license for evaluation purposes or the core can be made available on the Elliptic evaluation system – the EVAL-01.

Embedded Software Support

Elliptic will release in the second quarter of 2006 an embedded software solution - the ESW-01, which facilitates demonstration of a DTCP design in a video distribution application. The software is intended to be used as a demonstration of DTCP capabilities in conjunction with a target DTCP SoC or to be incorporated into a reference design that can be sub-licensed to end users. The ESW-01 has been implemented initially on a PC running Linux and will be ported to iTRON in line with the planned release date. The following diagram illustrates the software capabilities of the ESW-01.



More information is available to DTCP licensees by contacting:

Elliptic Semiconductor Inc.
308 Legget Dr., Suite 202
Kanata, ON, K2K 1Y6

Phone: +1 613 254-5456
Fax: +1 613 254-7260
Email: info@ellipticsemi.com