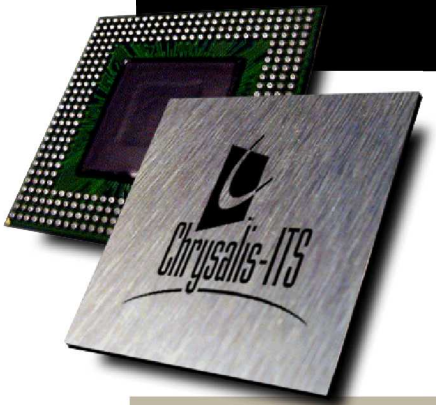
NETWORK SECURITY PROCESSOR

Luna® 340

ADVANCED DATA SHEET

Chrysalis-ITS®
ULTIMATE **TRUST** FOR PLANET e™



INTRODUCTION

The Luna® 340 series is a family of flexible, high performance integrated network security processors supported by an extensive development suite including algorithm libraries, drivers and API. Luna 340, which employs multiple optimized RISC cores, leverages Chrysalis-ITS expertise in trusted systems and cryptographic processing to provide an overall solution that reduces time-to-market. Cryptographic algorithms and protocols can be seamlessly offloaded providing hundreds of times performance improvement. Flexibility means that systems can be quickly upgraded to take advantage of changes to security protocols or evolving standards. Dual PCI buses double throughput and enable both a flow-through and co-processor architecture.

The Luna 340 supports a comprehensive set of algorithms and protocols. In addition, the Luna 340 is capable of supporting the new AES (Advanced Encryption Standard).

An evaluation board and software development kit are offered in the Luna NSP development platform. The development platform allows designers to interface with the Luna 340 at the application layer and take advantage of a wide range of layer 2 and 3 security protocols, asymmetric/symmetric cryptographic algorithms and packet processing functions.

The Luna 340 architecture is highly scaleable allowing Chrysalis-ITS to offer a range of devices to meet performance requirements in various systems while maintaining the same development platform to build on customers software investment.

Product Highlights

- Extensive software tools and development environment
- Integrated Secret and Public Key encryption processing
- Multi-Protocol support
- Parallel processors utilizing embedded RISC cores with optimized cryptographic instructions
- Control CPU
- Dual PCI 2.2 compliant 32-bit 66 MHz PCI buses
- PCI host and bus mastering functionality
- Global memory
- Phase Locked Loop
- Expansion port for external memory

Typical Applications

- E-Commerce Servers
- Web Switches
- Mid and Hi-range Routers
- Remote Access Servers
- Multi-service Access Routers
- Cable head-end systems
- Wireless access equipment
- Asynchronous Transfer Mode equipment

Technical Specifications

Performance:

IPSec-ESP (3DES-CBC/MD5) at 150Mbps

Bulk DES encryption up to Gigabit Ethernet rates

>100,000 security associations

300 RSA S/S @ 1024 bit key

205 IKE SA tunnel-setups/sec, 205 SSL sessions/sec

RC4 200Mbps

MD5 200 Mbps

SHA-1 180 Mbps

3DES 600 Mbps

Encryption algorithms supported:

DES, 3DES, RC2, RC4, RC5, RC6, MARS, Rijndael*, Serpent, Twofish, Blowfish, CAST, IDEA, MD2, MD4, MD5, SHA-1, RIPE-MD(128 and 160), HMAC-MD5, HMAC-SHA-1, RSA, DSA, Diffie-Hellman, ECDSA (over GF(p) and $GF(2^n)$), ECC (over GF(p) and $GF(2^n)$), Esign, ElGamal, GSM A3, A5 & A8.

Protocols supported:

IPSec (AH & ESP), IKE, MPPE, L2TP, SSL v2 and v3, TLS, SKIP, SMIME, SET, PPP DES and 3DES, PPP CHAP, Microsoft CHAP v1 and v2, SPKM, SSH, RADIUS, ATM Security Specification 1.0

Global Features:

IEEE 1149.1 JTAG interface

Built-in-self-test for memory testing

Real time clock

On-chip programmable PLL

304 contact thermal enhanced BGA package

Security Features:

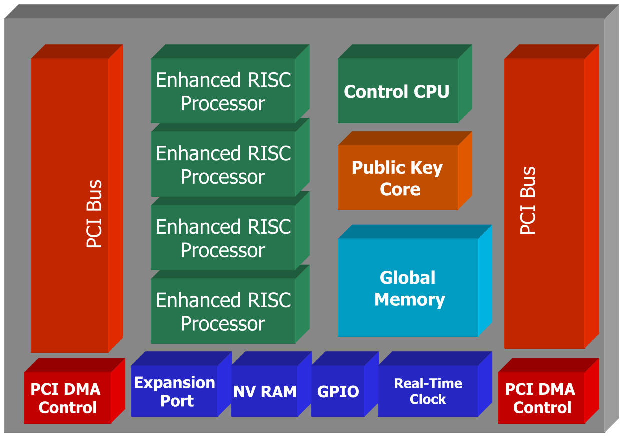
Random noise source input for internal ANSI X9.17 random number generator

Zeroize circuitry

Battery backed NVRAM for optional secure boot

Facilitates FIPS 140-1 Level 3 security validation

Luna® 340 Block Diagram



* Note: AES standard

Contact Information

For all inquiries about Chrysalis-ITS products please contact Chrysalis-ITS at:

Canadian Head Quarters		Ottawa ON:	(613) 723-5077
U.S. Offices			
Mountainview CA :	(650) 316-3622	Watertown MA :	(617) 926-9375
Norwell MA :	(781) 681-9542	Warrenton VA :	(540) 351-0700

Local support is provided in the locations listed in our web site at:
www.chrysalis-its.com

Chrysalis-ITS®
ULTIMATE **TRUST** FOR PLANET e™