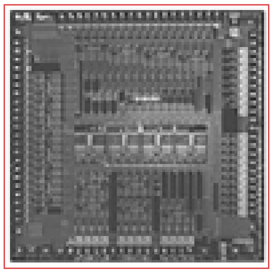
BROADCOM®

BCM5850

PRODUCT Brief



BCM5850 SSL/TLS RECORD LAYER PROTOCOL PROCESSOR

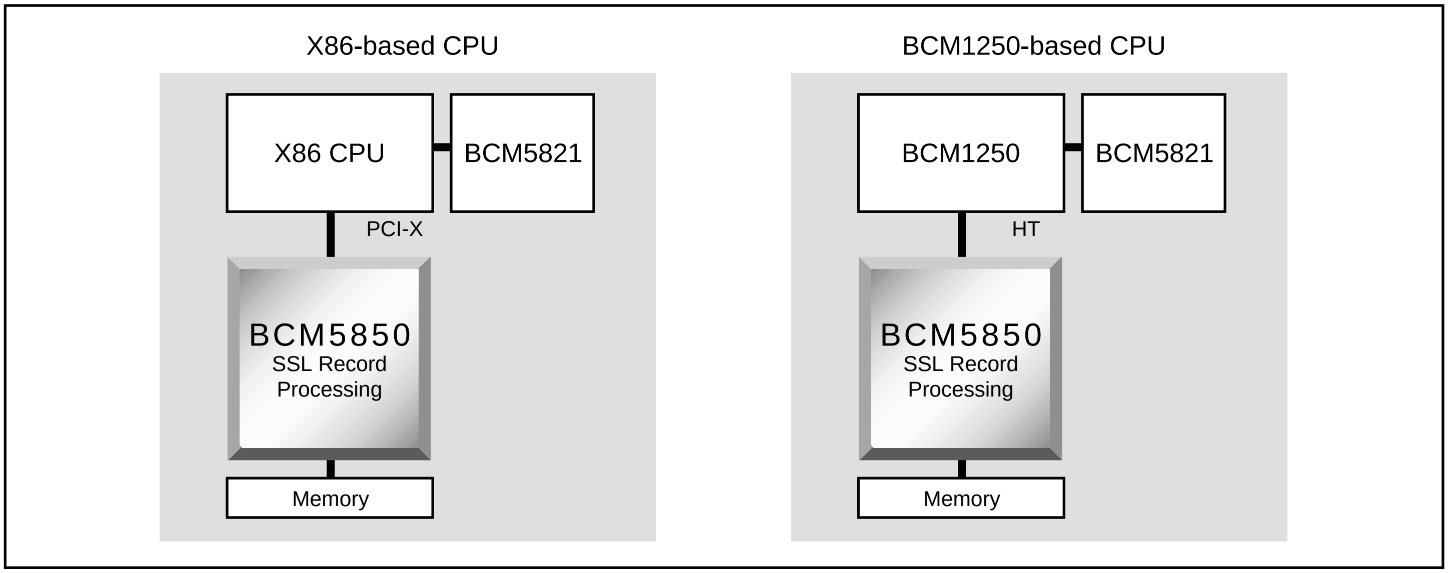
BCM5850 FEATURES

- **World's fastest SSL/TLS record processing**
  - 2.4 Gbps sustained data transfer throughput
  - Supports up to 20,000 complete handshakes/second
- **Advanced protocol processing**
  - Single pass SSLv3 or TLSv1 record processing
  - Support for SSLv2 record processing
  - Full key derivation for SSLv2, SSLv3, and TLSv1
  - Finished message processing for SSLv3 and TLSv1
  - Client certificate verify for SSLv3 and TLSv1
- **Local state storage**
  - 0-512 MB attached DDR SDRAM
  - Accessed and updated for each record
- **IETF and FIPS compatible algorithms**
  - 3DES-CBC, DES-CBC, DES40-CBC
  - ARCFOUR (40-bit, 56-bit, 128-bit)
  - NULL
  - AES-CBC (128-bit block—128, 192 and 256-bit keys)
  - MD5, SHA-1, MD5-HMAC, SHA-1-HMAC
  - TLSv1 PRF
- **High performance interfaces**
  - PCI-X 1.0, 32/64 bit 33/66 MHz PCI 2.2
  - 400 MHz 8-bit single-end Hyper Transport (HT)
- **Package**
  - 480-pin EBGA
- **Technology**
  - 0.18µ low power CMOS

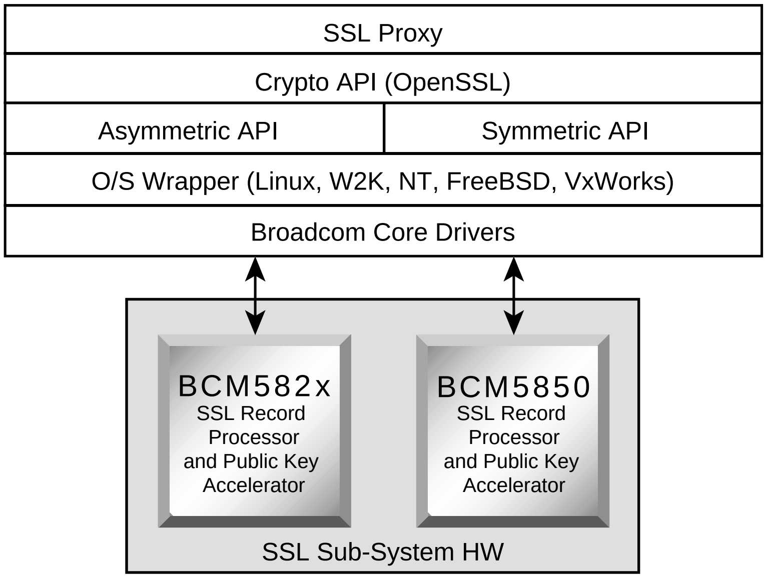
SUMMARY OF BENEFITS

- **Enables maximum system performance SSL/TLS proxy termination and web server acceleration**
  - Offloads compute intensive operations to hardware
  - Provides direct interface to state memory
- **Extensive software eases system integration**
  - Complete, multi-platform driver support
  - High level protocol function API
  - All libraries provided with portable source code
  - Future proof with common SSL software roadmap
- **Flexible interfaces allow rapid development**
  - Hyper transport provides seamless IF to broadband processors
  - PCI-X, PCI for server platform
- **Highest performance SSL processing enables security in high-bandwidth applications**
  - Load balancers
  - Layer 4-7 switches
  - SSL appliances
  - Caching appliances
  - Chassis based servers
  - Web servers/proxies
- **Scales to large systems without degradation**
  - Supports low overhead context switching
  - Supports hundreds of thousands of concurrent connections

SSL Applications Using the BCM5850



BCM5850 Overview


SSL Proxy
Crypto API (OpenSSL)
Asymmetric API
Symmetric API
O/S Wrapper (Linux, W2K, NT, FreeBSD, VxWorks)
Broadcom Core Drivers
BCM582x
SSL Record Processor and Public Key Accelerator
BCM5850
SSL Record Processor and Public Key Accelerator
SSL Sub-System HW

Broadcom BCM5850 and BCM582x Common API

The Broadcom **BCM5850** is a breakthrough chip that delivers new levels of SSL/TLS processing performance to secure web servers, proxy servers, and high-speed networking equipment that process SSL/TLS encrypted data. Designed to work in conjunction with the BCM 582x family of PCI Security Processors, the **BCM5850** provides direct APIs to accelerate processing of industry standard, compute intensive protocol operations:

- SinglePass record processing
- Session key derivation
- Finished message processing
- Client certificate verification

The **BCM5850** software APIs provide software compatibility with Broadcom's BCM582x Public Key Processing ICs. In addition to unlocking additional performance improvements in SSL/TLS Web Servers and Proxy Servers that offload public key operations using the BCM582x chips, the **BCM5850** allows rapid development and deployment of complete systems utilizing OpenSSL through the use of the Broadcom supplied Software Reference Library (SRL) and OpenSSL patches for the **BCM5850** APIs.

The **BCM5850** is available for evaluation in a PCI-X, PCI compatible card form factor for x86 based systems, and in a Hyper Transport (HT) based form factor for direct connection to Broadcom's broadband processor family's reference designs (i.e., BCM1250 and BCM112x).

The **BCM5850** PCI and HT evaluation cards support from 0–512 MB of DDR SDRAM memory via add-in DIMM memory modules.

The **BCM5850** is able to sustain throughputs of 2.4 Gbps using the ARCFOUR stream cipher or the 3DES, DES or AES block ciphers. The local attached memory allows hundreds of thousands of connections to have their cryptographic and protocol processing state accessed directly by the **BCM5850** processor, with no host processor memory penalty.

The **BCM5850** can support any combination of SSL/TLS traffic workload, from short duration e-commerce connections to longer duration file transfers using maximum size (16-KB) records.

The **BCM5850** provides the flexibility for all SSL/TLS systems and applications. The **BCM5850** has native hardware interfacing and software support for Broadcom's family of Broadband Processors (BCM1250, BCM112x).

Advanced tools and reference designs provided by Broadcom demonstrate the levels of SSL/TLS system performance that can be achieved using the **BCM5850**.

For more information please contact us at:
Phone: 949-450-8700, FAX: 949-450-8710
Email: info@broadcom.com

Visit our web site at: www.broadcom.com

BROADCOM CORPORATION
16215 Alton Parkway, P.O. Box 57013
Irvine, California 92619-7013