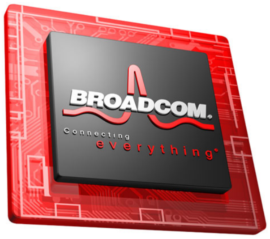
BROADCOM®

Connecting
everything®

BCM5821 PRODUCT Brief



SUPER E-COMMERCE PROCESSOR

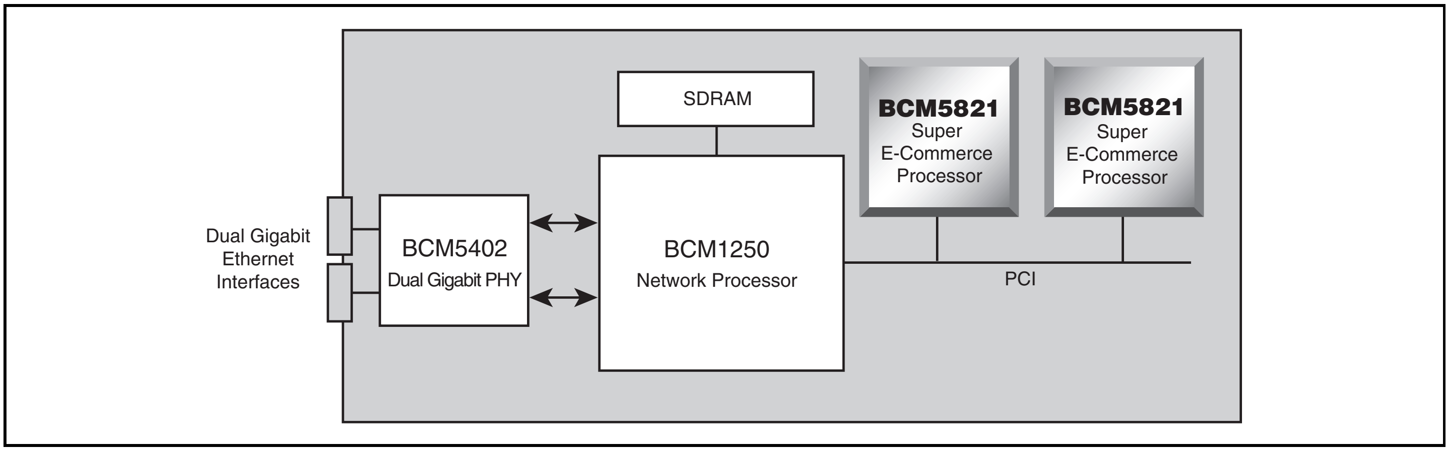
FEATURES

- **High-performance public-key processor**
  - 4000 1024-bit RSA transactions per second
  - 3000 Diffie-Hellman transactions per second
  - HW supports 1024- and 2048-bit RSA keys
  - Support for SSL/TLS and IKE modes
- **Integrated symmetric key processor**
  - DES, 3DES, ARC4, HMAC-SHA-1, HMAC-MD5
  - 470-Mbps IPsec (3DES, HMAC-SHA-1)
  - 600-Mbps ARC4
  - Supports unlimited number of simultaneous sessions
  - Full performance with different session for each packet
- **Concurrent public-key and symmetric-key processing**
- **Software and package compatible with BCM5820**
- **True hardware random number generator**
- **Optimized PCI interface**
  - PCI 2.2 interface, 32/64-bit, 33-66 MHz
  - Increased DMA block transfers
  - Optional EEPROM interface to configure PCI registers
- **125-MHz operating frequency**
- **0.18m CMOS technology, 1.8V core, 3.3V I/O**
- **Low power consumption: 2.8W**
- **256-TBGA package**

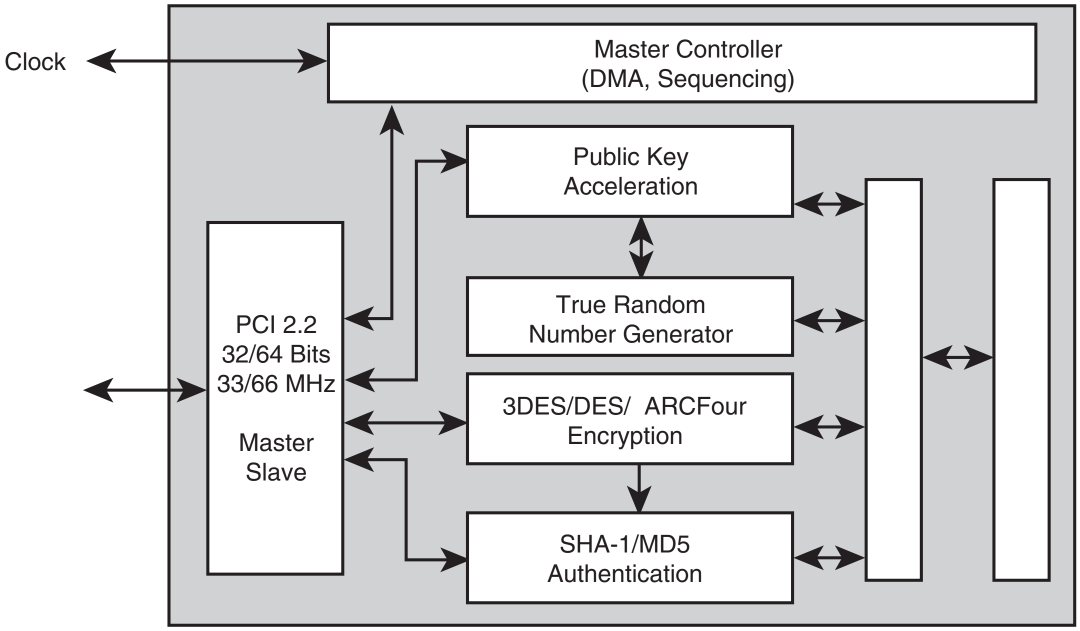
SUMMARY OF BENEFITS

- **Highest performance public key processor enables secure web transactions in embedded applications**
  - SSL appliances
  - Load balancers
  - Web/content switches
  - Web servers
- **Enable fast IKE negotiations for VPN applications**
  - VPN appliances
  - Edge routers
  - Access devices
  - Firewalls
- **High-performance SSL accelerator dramatically improves cost of SSL transactions per second**
- **Improves SSL performance and reduces delays associated with secure Internet transactions**
  - Increases SSL termination capacity
  - 4000 SSL handshakes per second
  - 20x the SSL performance over software solutions
- **Extensive embedded software development kit (SDK)**
  - VxWorks®, Linux®, BSD® support
  - Software reference library
  - Complete reference design
- **Concurrent processing minimizes latency on public-key and symmetric-key operations**
- **Integration reduces footprint and power consumption for embedded applications**
  - Over 1400 SSL sessions per watt

SSL Appliance Architecture



OVERVIEW


Clock
Master Controller (DMA, Sequencing)
Public Key Acceleration
True Random Number Generator
3DES/DES/ ARCFour Encryption
SHA-1/MD5 Authentication
PCI 2.2
32/64 Bits
33/66 MHz
Master
Slave

The BCM5821 Super E-commerce processor is a high-performance public-key processor, able to perform over 4000 SSL/TLS sessions per second and 3000 IKE negotiations per second. The high level of performance and integration in the BCM5821 makes it ideal for high-performance embedded applications with footprint and power limitations.

In addition to its high-performance public-key engines, the BCM5821 offers acceleration for symmetric key functions at increased performance rates. The BCM5821 supports bulk SSL encryption and authentication (ARC4, SSL-MAC-MD5/SHA-1) in-system performance at 300 Mbps and IPsec (3DES, HMAC-SHA-1) in-system performance at 470 Mbps.

A true hardware random number generator on the BCM5821 is well suited for IV seeding and secret key generation.

For SSL applications, a single BCM5821 can support 4000 SSL sessions per second, thus dramatically improving the response time of load balancers, Web switches, servers, and SSL appliances. For IKE applications, the BCM5821 can initiate 3000 VPN tunnels per second.

The BCM5821 device's PCI interface makes it a perfect solution for all cost-sensitive security applications. Requiring no external components, the BCM5821 is ideal for embedded applications with strict board space and power requirements. Furthermore, performance of the BCM5821 can easily be scaled to increase both public-key and bulk payload processing performance.

Unlimited security association (SA) support via system memory and a multi-threaded DMA engine utilizes system memory to maximize throughput in real-world applications. The ability to prefetch packet contexts minimizes the performance degradation when processing small packets. Concurrent public-key and bulk payload processing minimizes latency and improves system performance dramatically.

Application program interface (API) support through Broadcom's Software Reference Library (SRL) for IPSec and SSL application software offers BCM5821 users a complete system solution. The BCM5821 SDK includes support for VxWorks, Linux and BSD.

Connecting everything®

BROADCOM®

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

Phone: 949-450-8700
Fax: 949-450-8710
E-mail: info@broadcom.com
Web: www.broadcom.com