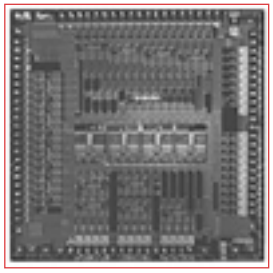
BROADCOM®
Connecting everything™

BCM5820
PRODUCT Brief



BCM5820 E-COMMERCE PROCESSOR

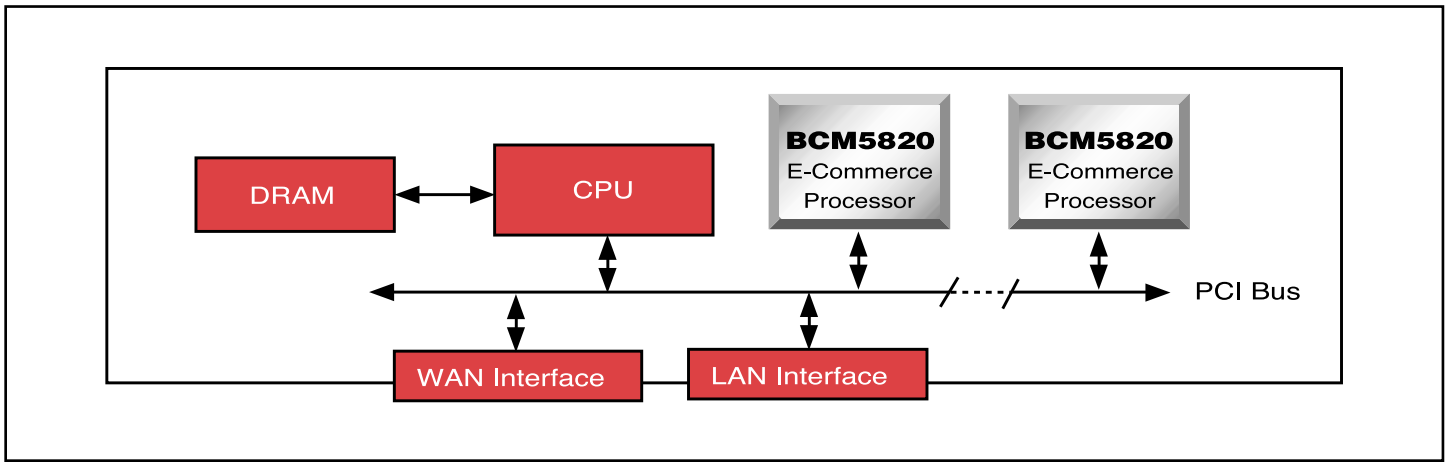
BCM5820 FEATURES

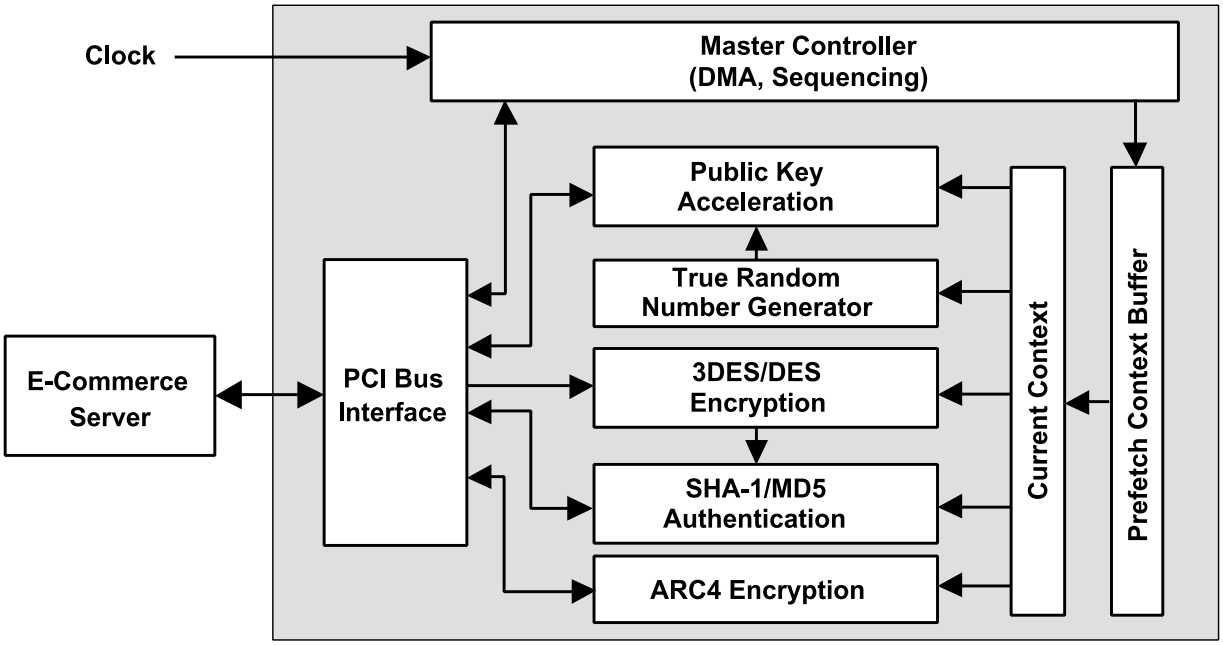
- **World's fastest integrated security processor for e-commerce SSL and VPN IKE applications. World's fastest integrated public-key setup processor includes:**
  - 1250 Diffie-Hellman key exchange pairs per second
  - 800-bit RSA private key signings per second
  - Hardware support for 2,048-bit keys
  - Extensive support for all SSL, TLS and IKE modes
- **Integrated symmetric cryptography processor**
  - Support for IPSec and SSL/TLS payload processing
  - Single-pass IPSec encryption and authentication
  - 310 Mbps IPSec (3DES + MD5/SHA1)
  - 200 Mbps ARC4 Processing
  - Support for unlimited number of simultaneous sessions
  - Full performance with a different session for each packet
- **Integrated true hardware random number generator**
- **Optimized pre-fetching PCI interface**
  - Full performance maintained independent of any reasonable PCI latency
  - PCI 2.2 interface, 32/64 bits, 33-66 MHz
- **0.22m CMOS technology, 2.5V core, 3.3V I/0**
  - Low-power design
- **256-TBGA**

SUMMARY OF BENEFITS

- **Incorporates all the functions of competitive board-level solutions at a fraction of the cost.**
  - 800 RSA transactions per second, 4 – 5x the speed of competitive boards
  - Integrated chip can reduce price point of SSL accelerators from thousands to hundreds of dollars
- **Reduces delays associated with secure e-commerce transactions.**
  - Accelerates SSL protocol used in all web browsers
    - Standard in Internet Explorer and Netscape Navigator
    - Uses RSA encryption; Compute intensive operation
    - 4x the SSL connections per second of software-based web servers
- **Features software-scalable architecture.**
- **Software compatible with BCM5805.**
- **Extensive software and systems support.**
  - Software reference library supports popular e-commerce servers (Open SSL, Microsoft IIS, iPlanet/Netscape, PKCS-11)
  - Complete reference design
  - FIPS 140-1 support
  - Multi-platform driver support:
    - Linux,Win98,Win2000, FreeBSD, VxWorks, Solaris
- **Flexible e-commerce and VPN solution.**
  - E-commerce servers
  - SSL proxy for web switches, load balancers
  - SSL and VPN appliances

SSL/TLS E-Commerce Server Diagram





The **BCM5820** integrates into a single 256-BGA package 4–5x the public key performance of competing board level products at a fraction of the cost. The **BCM5820**'s 32/64 33-66 MHz PCI interface makes it a perfect solution for add-in card applications for high performance e-commerce servers, load balancing and web switching equipment.

The **BCM5820** offers full-duplex OC3 IPSec processing (310 Mbps-3DES, HMAC-SHA-1) performance, and in excess of 1250 Diffie-Hellman transactions per second (1024-bit public key, 160-bit private key) and 800 RSA private key signings per second. The **BCM5820** is also ideal as a high performance VPN IKE coprocessor in Internet infrastructure aggregation equipment.

The highly integrated **BCM5820** E-Commerce Processor is the ideal solution for offloading compute intensive SSL operations in e-commerce servers and networking products such as web switches and load balancing devices. Extensive hardware support for processing intensive public key operations, minimizes the user software required for IKE and SSL/TLS key negotiations. The **BCM5820** is also software-compatible with the BCM5805 e-commerce processor.

The **BCM5820** e-commerce processor integrates the industry's highest-performance single-chip public key processing unit, 200–Mbps ARC4 engine, true random number generator, high-performance IPSec engine (DES, 3DES, HMAC-SHA-1, HMAC-MD5), and 64/66 PCI interface all in a single chip configuration.

Requiring no external components, the performance of **BCM5820** system can easily be scaled by adding more **BCM5820** chips in board-space-sensitive rack-mount equipment. An aggressive pre-fetch DMA eliminates the need for external memory and maximizes throughput under real-world conditions.

API support through Broadcom's Software Reference Library (SRL) for SSL and IPSec application software offers **BCM5820** users a whole product solution. Compatibility with Open SSL, Microsoft IIS, iPlanet/Netscape, PKCS-11, Novell and industry leading IPSec software from SSH Communications eases integration and reduces time to market.

Connecting everything™

BROADCOM®

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

Phone: 949-450-8700
FAX: 949-450-8710
Email: info@broadcom.com
Web: www.broadcom.com

5820-PB02-R-3.5.02