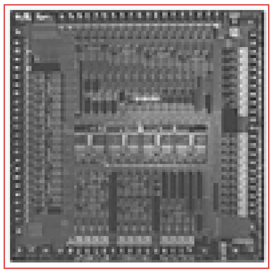
BROADCOM®

Connecting everything™

BCM5802
PRODUCT Brief



BCM5802 SECURITY PROCESSOR

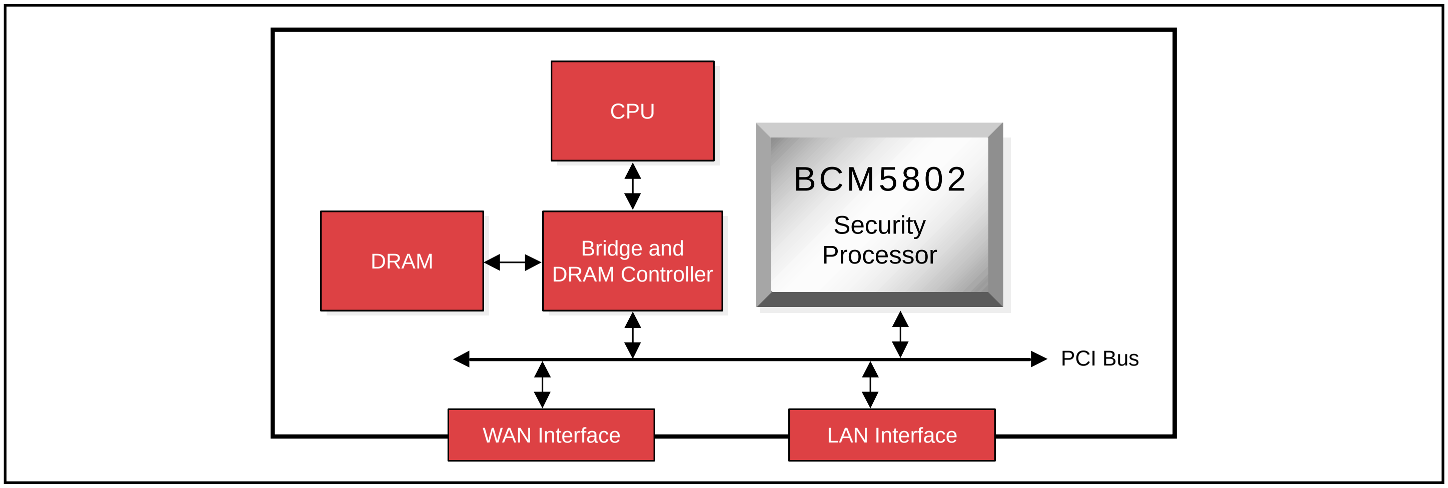
BCM5802 FEATURES

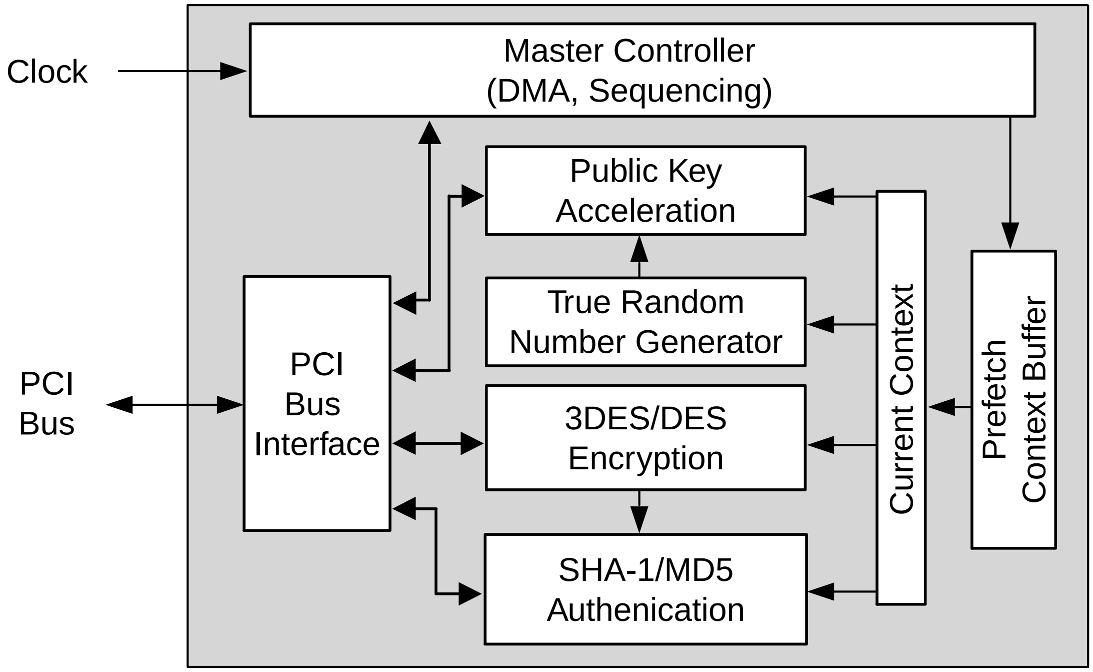
- **Feature rich single-chip security processor integrating full IPSec and IKE acceleration**
- **Supports DES, 3DES, HMAC- SHA-1 and HMAC-MD5**
- **100 Mbps IPSec (3DES, SHA-1) "In-System" performance, with new Security Association (SA) per packet**
- **Sustainable 50 Mbps on 200-byte packets**
- **Unlimited SA support via system memory**
- **Extensive hardware acceleration support for IKE/SSL/TLS key setup**
- **Public key acceleration unit supports 30 Diffie-Hellman key exchanges per second**
- **True hardware random number generator**
- **Supports multi-packet processing and pre-fetch of packet data and context**
- **Multi-threaded DMA allows multi-packet processing with a single PCI write**
- **Accommodates most PCI latency problems without performance degradation**
- **PCI 2.2 interface, 32 bits, 33 MHz**
- **33 MHz operating frequency**
- **Low-power 3.3V design**
- **144-pin DQFP package**

SUMMARY OF BENEFITS

- **Highly integrated security processor**
  - Single-chip IPSec, IKE, SSL/TLS accelerator
  - Multi-threaded DMA engine
  - True hardware random number generator
  - On-chip context buffer memory
  - Lowest system cost
- **Sustainable performance in real-world conditions**
  - DMA supports multi-packet processing
  - Pre-fetch of new context and packet
- **Flexible, easy to use PCI 2.2 interface**
  - No external components required
  - Ideal for low-cost, add-in card applications
  - Compatible with all existing PC systems
- **Whole product solution minimizes time-to-market**
  - Software Reference Library (SRL) includes a hardware abstraction software layer
  - Compatible with industry standard SSH IPSec and IKE software
  - Compatible with OpenSSL
- **Flexible VPN solution for all data security applications**
  - VPN appliances
  - Small office VPNs
  - DSL modems

SOHO VPN System Diagram





The **BCM5802** Security Processor integrates Broadcom's IPSec engine (DES, 3DES, HMAC-SHA-1, HMAC-MD5), public key processor, true random number generator, PCI interface and context buffer memory onto a single chip. The **BCM5802** Security Processor is an ideal solution for DSL modems, VPN-enabled networking products such as SOHO routers, gateways and VPN appliances.

The **BCM5802** combines performance and cost optimization for applications requiring hardware assist for MIPS intensive IPSec and IKE processing. Accelerating bulk cryptographic functions (DES, 3DES, SHA-1 and MD5) and public key operations, the **BCM5802** includes extensive hardware support for processing intensive public key operations and minimizes the user software required for IKE and SSL/TLS key negotiations.

The **BCM5802** provides 100 Mbps performance and in excess of 30 Diffie-Hellman key exchanges per second (1024-bit public key, 180-bit private key). IPSec performance is measured "in-system" on outbound packets, with new security associations per packet.

A true hardware random number generator on the **BCM5802** is well suited for IV seeding and secret key generation.

The **BCM5802's** PCI interface makes it a perfect solution for all cost-sensitive security applications. Requiring no external components, the **BCM5802** is ideal for add-in card applications requiring IPSec acceleration. 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 pre-fetch packet contexts minimizes the performance degradation when processing small packets.

Application program interface (API) support through Broadcom's Software Reference Library (SRL) for IPSec and SSL application software offers **BCM5802** users a complete system solution. Compatibility with OpenSSL and industry standard 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