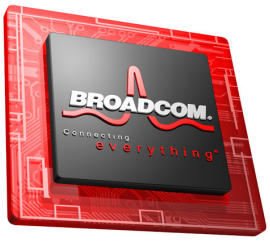
BROADCOM®
Connecting everything®

BCM5801 PRODUCT Brief



CRYPTOGRAPHIC PROCESSOR

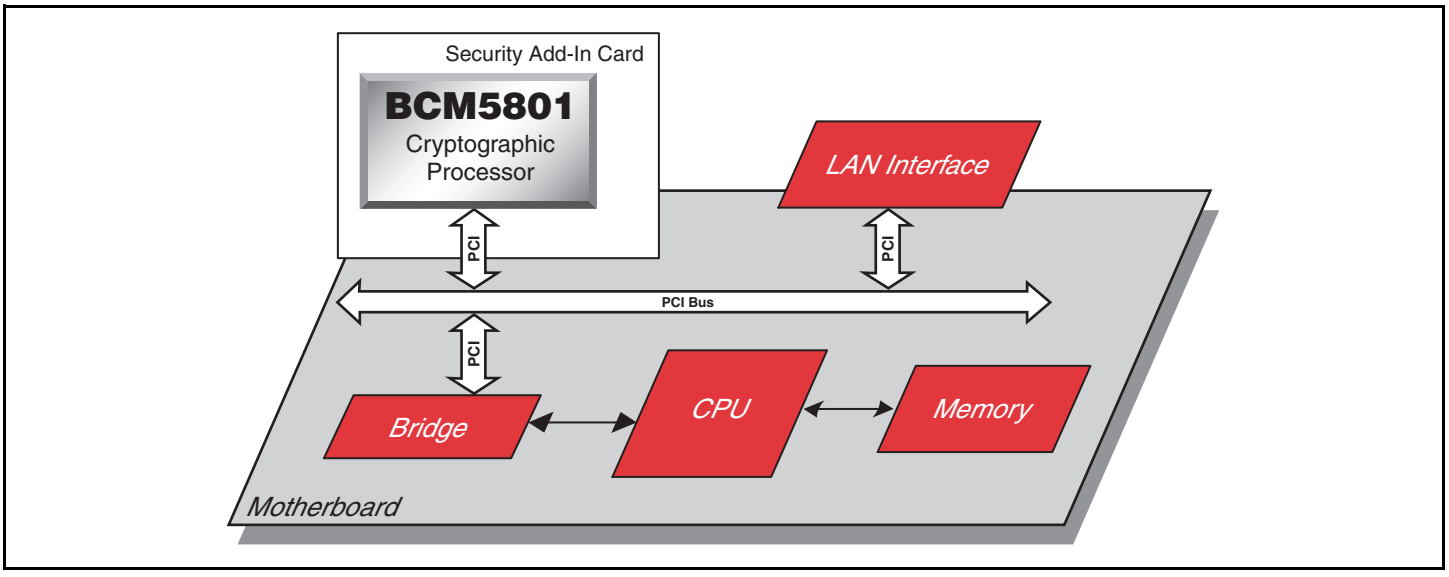
FEATURES

- **High-performance single-chip cryptographic processor**
- **Supports DES, 3DES, HMAC- SHA-1, and HMAC-MD5**
- **Single-pass encryption and authentication of packet data**
- **200-Mbps IPSec (3DES, SHA-1) in-system performance, with new Security Association (SA) per packet**
- **Unlimited SA support via system memory**
- **Compatible with SSH IPSec software**
- **Supports multi-packet processing and prefetch of packet data and context**
- **Multi-threaded DMA allows multi-packet processing with single PCI writes**
- **Accommodates most PCI latency problems without performance degradation**
- **66-MHz operating frequency**
- **PCI 2.2 interface, 32-bit, 33/66 MHz**
- **Low-power 3.3V design**
- **144-pin DQFP package**

SUMMARY OF BENEFITS

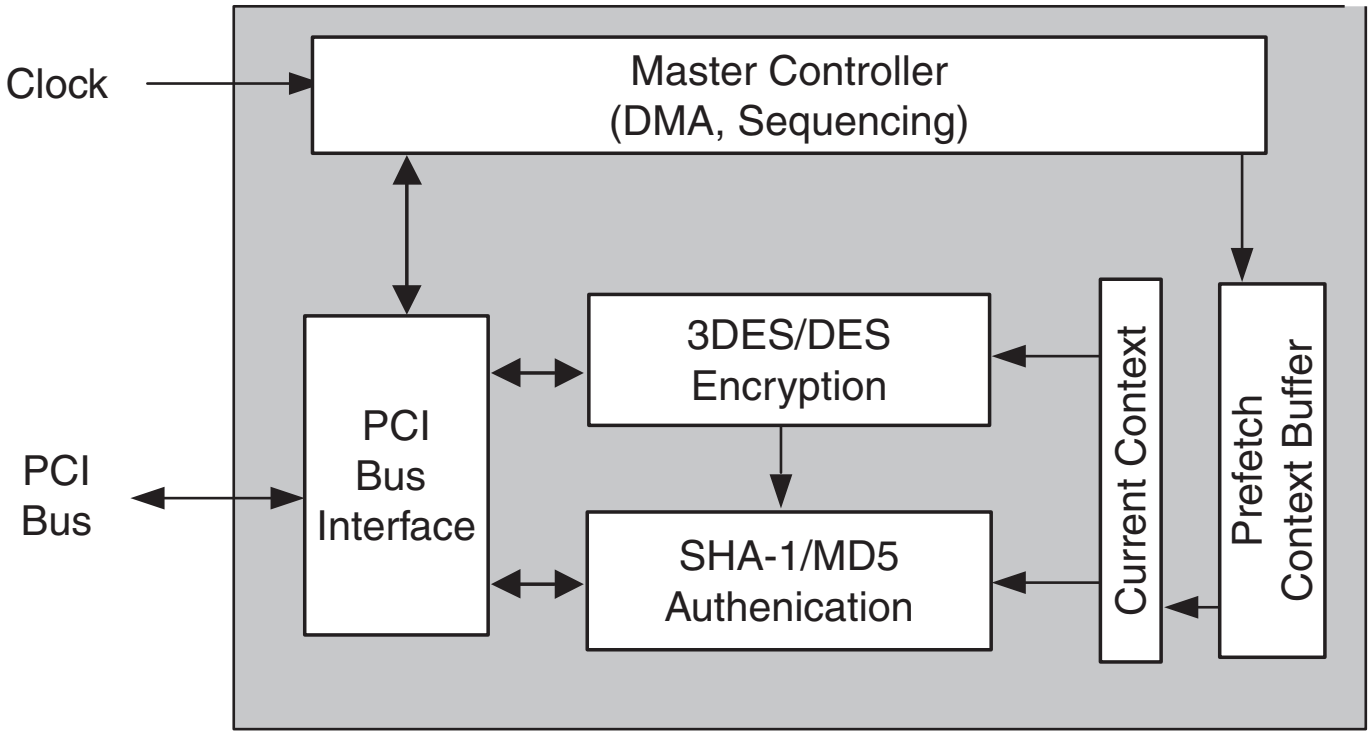
- **Low-cost, easy-to-design-single-chip security solution**
  - Smallest footprint
  - Lowest system cost
- **Sustainable real-world performance**
  - DMA supports multi-packet processing
  - Prefetch of new context and packet
- **Flexible, easy-to-use PCI 2.2 interface**
  - No external components required
  - Ideal for low-cost add-in card applications
  - Compatible with all existing PC systems
- **Complete product solution minimizes time to market**
  - Software Reference Library (SRL) including a hardware abstraction software layer
  - Compatible with industry-standard SSH IPSec software
- **Flexible VPN solution for all data security applications:**
  - Firewalls
  - VPN appliances
  - Client applications
  - IPSec acceleration

Cryptographic Add-In Card System Diagram



BROADCOM®

OVERVIEW



The BCM5801 cryptographic processor integrates a high-performance IPSec engine (DES, 3DES, HMAC-SHA-1, HMAC-MD5), PCI interface, and context buffer memory into a single chip. Ideally suited for cost-sensitive client applications, the BCM5801 cryptographic processor offers tremendous performance in a compact design. Offering hardware acceleration for IPSec cryptographic functions makes the BCM5801 an ideal solution for applications such as SOHO routers and gateways, firewalls, VPN appliances, and network interface cards.

The BCM5801 provides complete 200-Mbps IPSec processing (3DES, HMAC-SHA-1) performance in a highly integrated design. The BCM5801 offers a unique combination of performance and cost-optimization by integrating the necessary functional blocks into a single chip.

The BCM5801 device's PCI interface makes it a perfect solution for all cost-sensitive security applications. Requiring no external components, the BCM5801 is ideal for add-in card applications requiring IPSec acceleration. A multi-threaded DMA engine utilizes system memory to maximize throughput in real-world applications. Unlimited security association (SA) support via system memory, and the ability to prefetch packet contexts, minimize the performance degradation when processing small packets.

Application program interface (API) support through Broadcom's Software Reference Library (SRL) for IPSec application software offers BCM5801 users a complete system solution. Compatibility with industry-standard SSH IPSec software eases integration and reduces time to market.

Connecting everything®

BROADCOM®

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

5801-PB04-R 07/08/04

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