BROADCOM®

Connecting
everything®

BCM5812
PRODUCT Brief

SECURITY PROCESSOR

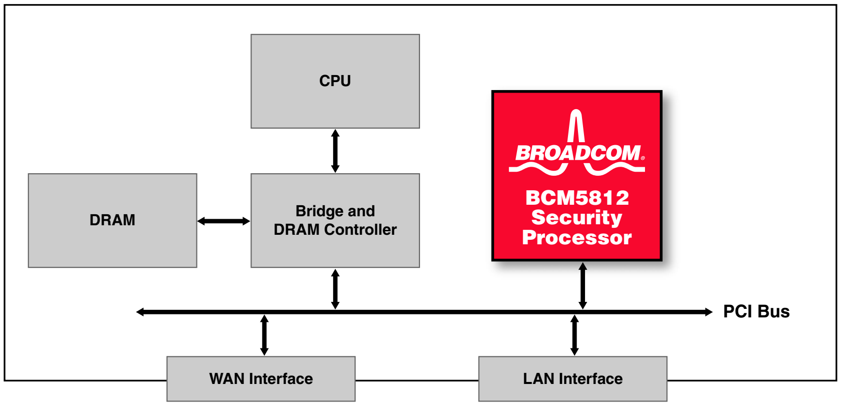
FEATURES

- **Feature-rich single-chip security processor integrating full-featured AES support**
- **50-Mbps system throughput**
  - DES-CBC, 3DES-CBC
  - AES-CBC, AES-CTR (up to 256-bit key lengths)
  - HMAC-SHA-1, HMAC-MD5
  - Single-pass encryption and authentication
- **Integrated public-key processor**
  - 50 Diffie-Hellman transactions per second
  - 65 1024-bit RSA transactions per second
  - Hardware supports 1024- and 2048-bit RSA keys
  - Support for IKE and SSL/TLS modes
- **Concurrent public-key and symmetric-key processing**
- **True hardware random number generator**
- **Software-compatible with the BCM580X and BCM582X**
- **Supports multi-packet processing and prefetch of packet data and context**
- **Multi-threaded DMA allows multi-packet processing with single PCI write**
- **Optimized PCI interface**
  - PCI 2.2 interface, 32-bit, 33 MHz
  - Optional EEPROM interface to configure PCI registers
- **0.18m-CMOS technology, 1.8v core, 3.3v I/O**

SUMMARY OF BENEFITS

- **Software-compatible solutions enables scalability across product families**
- **Improves security performance in cost-sensitive, low-power embedded applications**
  - SOHO routers
  - Low-end routers
  - VPN appliances
  - Firewalls
- **AES support provides latest algorithm support and protects against obsolescence**
  - 256-bit key length support of AES
- **Enables fast IKE negotiations for VPN applications**
- **Sustainable performance in real-world conditions**
  - DMA supports multi-packet processing
  - Prefetch of new context and packet
- **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**

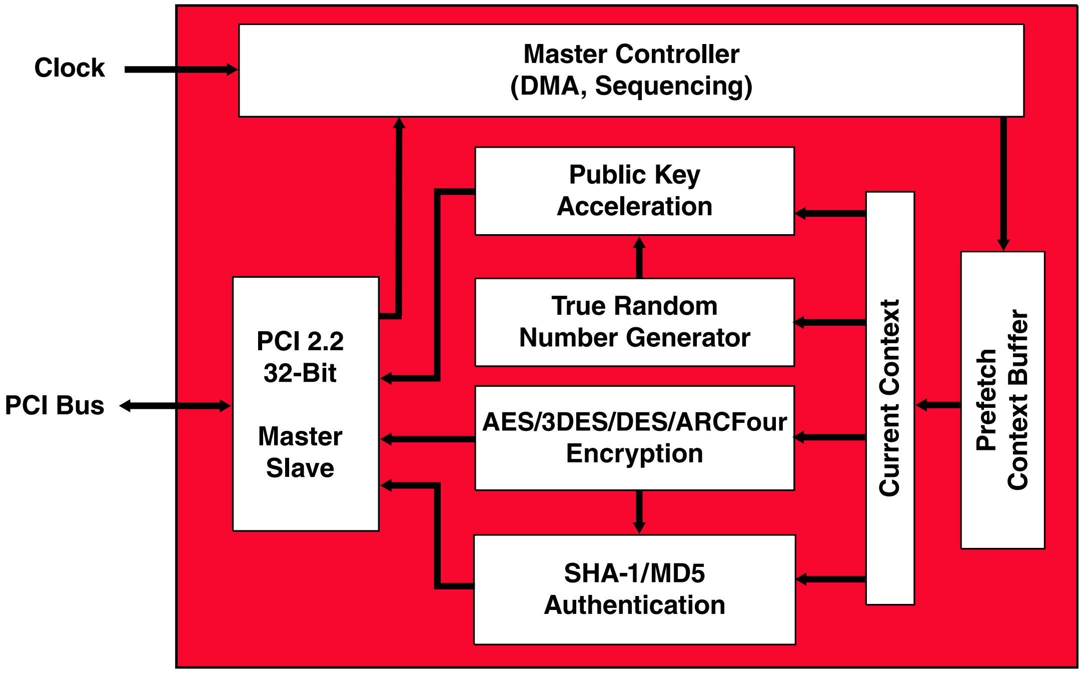
BCM5812 in VPN Applications



BROADCOM.

Downloaded from Elcodis.com electronic components distributor

OVERVIEW



BCM5812 Block Diagram

The BCM5812 complements the CryptoNetX™ family of security processors. Offering software compatibility with the BCM580X and BCM582X products, the BCM5812 allows customers to support performance from 50 Mbps to 1 Gbps with a common software platform.

The BCM5812 security processor is a fully integrated, cost-effective cryptographic processor capable of performing 50 Mbps of IPsec (3DES, HMAC-SHA-1) system throughput. The BCM5812 includes AES in its cryptographic engine with support of key lengths up to 256 bits. In addition to its full-featured symmetric key engine, the BCM5812 offers public-key acceleration for IKE processing at the rate of 50 Diffie-Hellman transactions per second. The BCM5812 security processor is an ideal solution for cost-sensitive applications requiring hardware acceleration with the latest cryptographic features.

The BCM5812 combines performance and cost optimization for applications requiring hardware assist for CPU-intensive IPSec and IKE processing. Accelerating bulk cryptographic functions (AES, 3DES, SHA-1, and MD5) and public-key operations, the BCM5812 includes extensive hardware support for processing intensive public-key operations and minimizes the user software required for IKE and SSL/TLS key negotiations.

A true hardware random number generator on the BCM5812 is well suited for IV seeding and secret key generation.

The BCM5812 device's PCI interface makes it a perfect solution for all cost-sensitive security applications. Requiring no external components, the BCM5812 is ideal for embedded applications with strict board space and power requirements. Furthermore, performance of the BCM5812 can easily be scaled to increase both IPsec and public-key processing performance.

Unlimited security association (SA) support via system memory and a multi-threaded DMA engine utilize system memory to maximize throughput in real-world applications. Able to prefetch packet contexts, this 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 BCM5812 users a complete system solution. The BCM5812 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