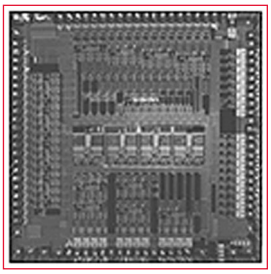
BROADCOM®
Connecting everything®

BCM5823
PRODUCT Brief



BCM5823 SECURITY PROCESSOR

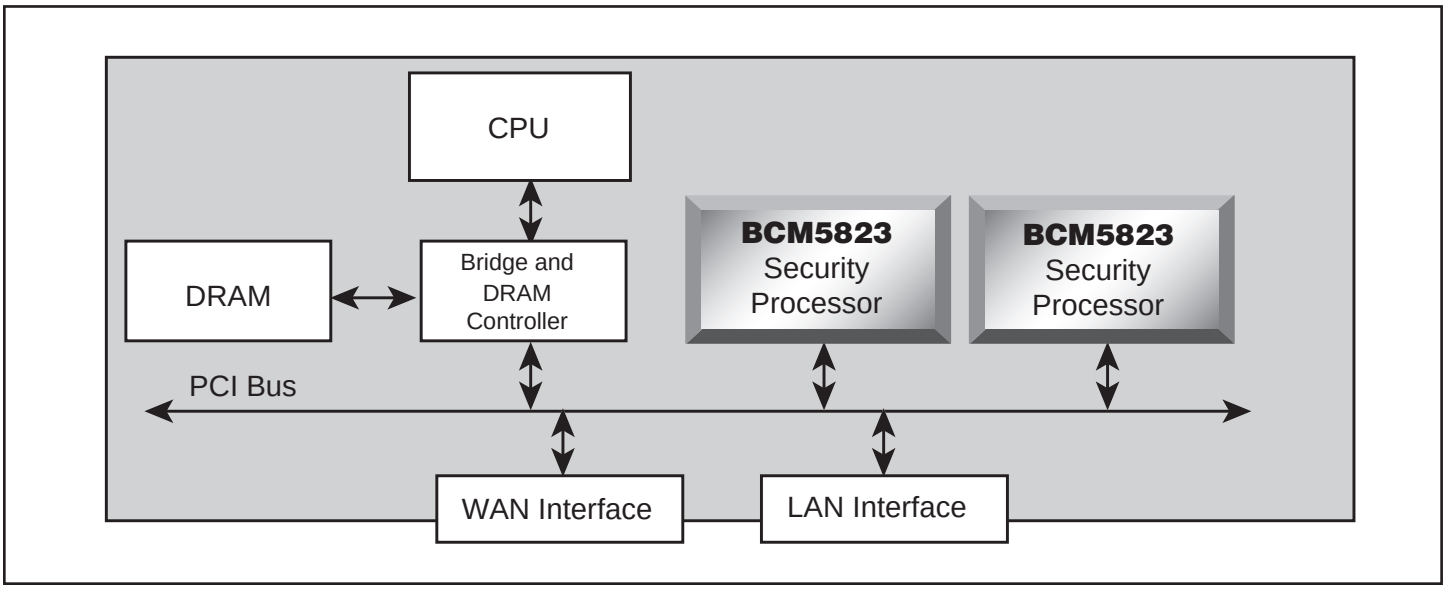
BCM5823 FEATURES

- **High-performance security co-processor**
- **500-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**
  - 400 Diffie-Hellman transactions per second
  - 550 1024-bit RSA transactions per second
  - HW supports 1024 and 2048 bit RSA keys
  - Support for IKE and SSL/TLS modes
- **Scalable to 1 Gbps of IPsec processing**
- **Concurrent public-key and symmetric key processing**
- **Software and package compatible with BCM5821**
- **True hardware random number generator**
- **Optimized PCI interface**
  - PCI 2.2 interface, 32/64-bit, 33-66 MHz
  - Optional EEPROM interface to configure PCI registers
- **133-MHz operating frequency**
- **0.18-µm CMOS technology, 1.8V core, 3.3v I/O**
- **Low power consumption: 1.3 W**
- **Package: 256 PBGA (27 x 27)**

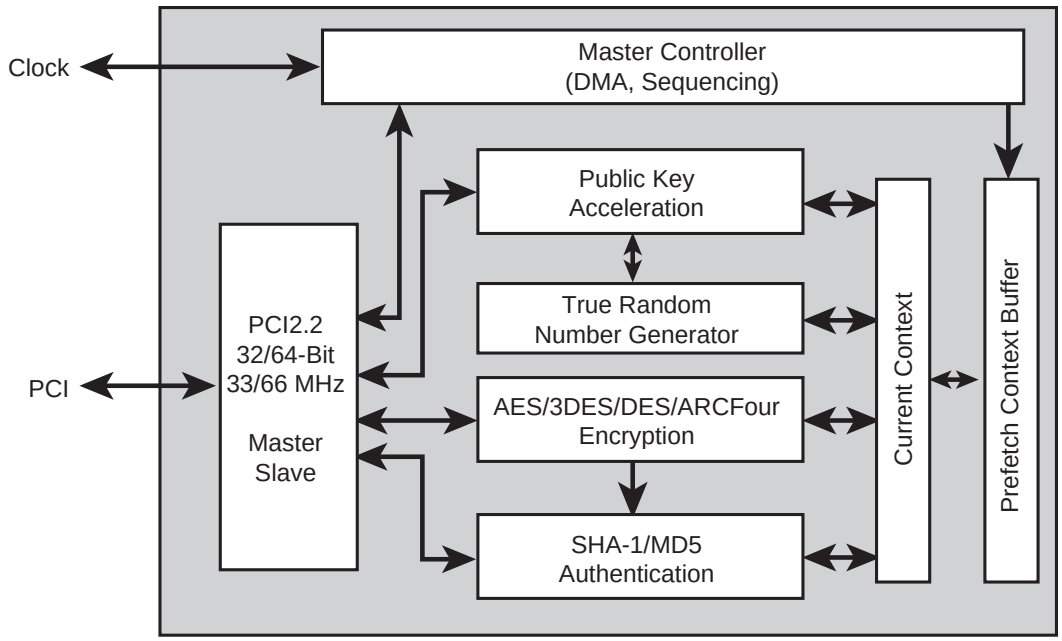
SUMMARY OF BENEFITS

- **Improves security performance in high-performance embedded applications**
  - Firewalls
  - VPN Appliances
  - VPN-Enabled Routers
  - Access Devices
- **AES support provides latest algorithm support and protects against obsolescence**
  - 256-bit key length support of AES
- **Scalability enables high-end architectures**
- **Two BCM5823s provide up to 1 Gbps performance**
- **Enables fast IKE negotiations for VPN applications**
- **Reduces load on host CPU for high-performance security processing**
- **Easy upgrade from BCM5821**
- **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**

BCM5823 in 1-Gbps VPN Application



BCM5823 OVERVIEW



The **BCM5823** security processor is a fully-integrated, high-performance cryptographic processor capable of performing 500 Mbps of IPsec (3DES, HMAC-SHA-1) system throughput. The **BCM5823** includes AES in its cryptographic engine with support of key lengths up to 256-bits. In addition to its high-performance symmetric key engine, the **BCM5823** offers public-key acceleration for IKE processing at the rate of 400 Diffie-Hellman transactions per second. The high level of performance and integration in the **BCM5823** makes it ideal for high-performance embedded applications with footprint and power limitations.

A true hardware random number generator on the **BCM5823** is well suited for IV seeding and secret key generation.

The **BCM5823** is ideal for high-end and mid-range firewall and VPN appliance applications. Able to scale to 1 Gbps with multiple devices, the **BCM5823** addresses a very broad range of performance points. Utilizing a common software base, customers can develop families of products with common architectures and software platforms.

The **BCM5823** device's PCI interface makes it a perfect solution for all cost-sensitive security applications. Requiring no external components, the **BCM5823** is ideal for embedded applications with strict board space and power requirements. Furthermore, performance of the **BCM5823** 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 utilizes system memory to maximize throughput in real-world applications. Ability to pre-fetch 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 **BCM5823** users a complete system solution. The **BCM5823** 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
Email: info@broadcom.com
Web: www.broadcom.com

5823-PB01-R 03.17.03