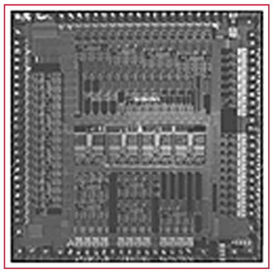
BROADCOM®

Connecting everything®

BCM5823 PRODUCT Brief



BCM5823 SECURITY PROCESSOR

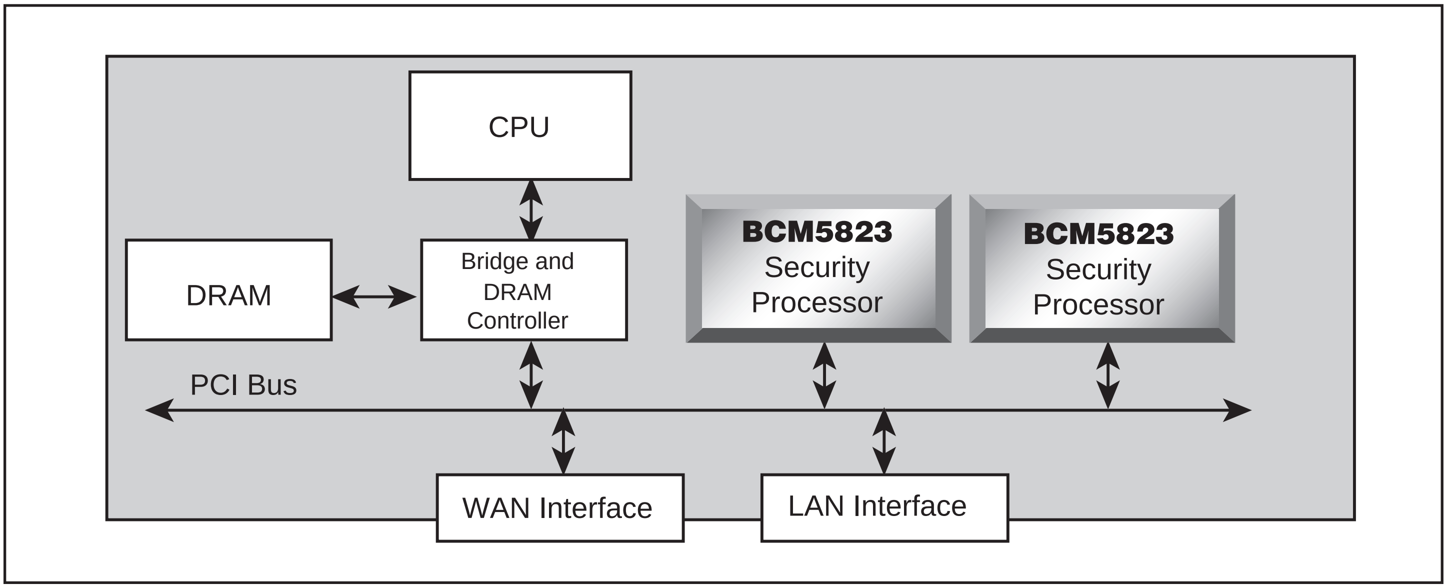
BCM5823 FEATURES

- **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-Enabled Routers
  - VPN Appliances
  - 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


CPU
DRAM
Bridge and DRAM Controller
BCM5823 Security Processor
BCM5823 Security Processor
PCI Bus
WAN Interface
LAN Interface