



## HIGH-PERFORMANCE SECURITY PROCESSOR

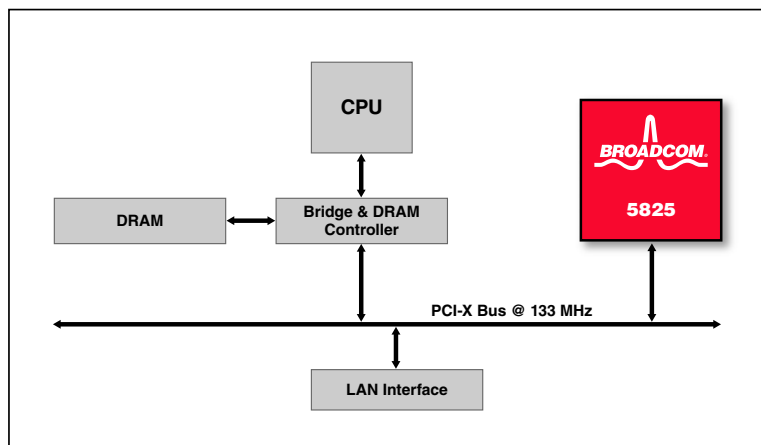
### FEATURES

- **High-performance VPN and SSL security processor**
  - 1-Gbps system throughput
    - AES-CBC, AES-CTR
    - DES-CBC, 3DES-CBC
    - HMAC-SHA-1, HMAC-MD5
    - Single-pass IPsec processing (encryption and authentication)
  - Integrated public key processor
    - 15,224 1024-bit RSA transactions per second
    - 15,224 Diffie-Hellman 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**
- **Software compatible with the BCM5823 and BCM5821**
- **True hardware random number generator**
- **Optimized PCI-X® interface**
  - 64-bit, 133-MHz PCI-X 1.0 interface
  - Backward compatible with PCI
  - Increased DMA block transfers
- **0.13-µm CMOS technology**
- **400-pin PBGA lead-free package**

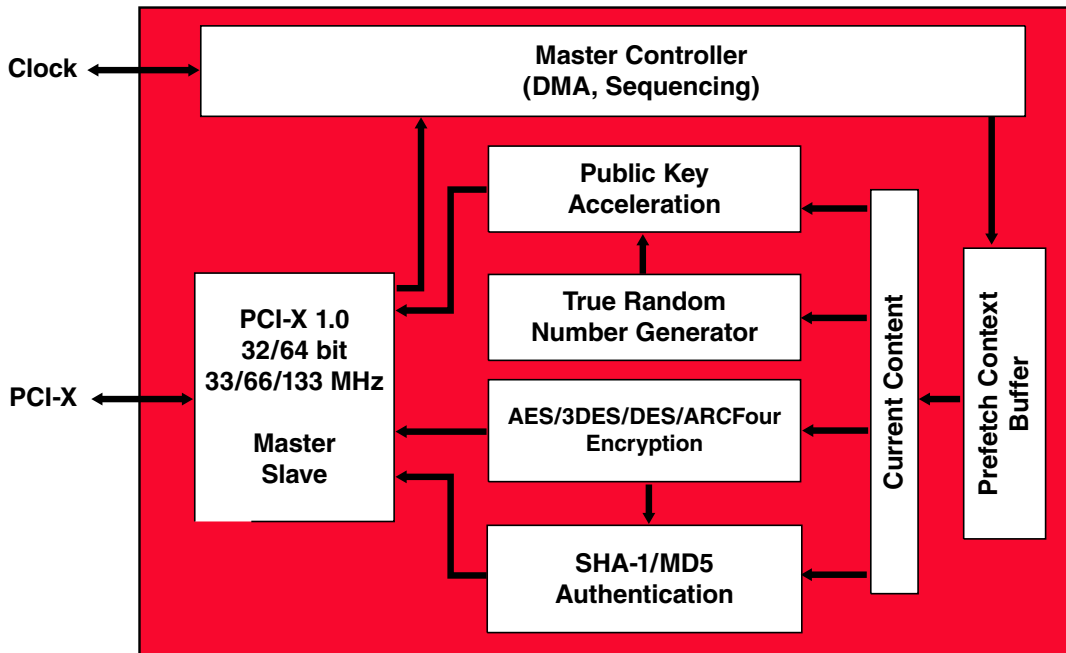
### SUMMARY OF BENEFITS

- **High-performance security coprocessor enables both secure web and high-performance VPN applications**
  - Web servers
  - Layer 4+ switches
  - Web appliances with integrated SSL
  - Access devices
  - Firewalls
  - VPN enabled routers
  - VPN appliances (IPsec/ SSL)
- **Extensive embedded software development kit**
  - Linux®, VxWorks®, and BSD® support
  - Software reference library
  - Full OpenSSL integration
  - Complete reference design
- **Easy upgrade from BCM5823 and BCM5821**
- **Compatible with other Broadcom devices, enabling optimal system-level form factor costs and power dissipation**
- **Enables use of one firewall and VPN system solution across different types of access equipment like appliances and routers deploying similar services**

### 1-Gbps VPN and 15,224 TPS SSL System Application



## OVERVIEW



**BCM5825 Block Diagram**

The BCM5825 security processor is a fully integrated, high-performance public-key and cryptographic processor capable of performing 15,224 RSA transactions per second, 15,224 IKE negotiations per second, and 1 Gbps of bulk AES and IPsec performance. The high level of performance and integration make it ideal for high-performance embedded VPN and SSL applications with footprint and power limitations.

For SSL applications, a single BCM5825 can support 15,224 SSL sessions per second, which dramatically improves the response time of layer 4+ switches, server load balancers, servers and other appliances with integrated SSL capability.

For VPN applications, the BCM5825 offers acceleration for symmetric key functions at significantly increased performance rates compared to legacy security products. The BCM5825 supports bulk AES encryption and authentication performance of 1 Gbps, bulk SSL encryption and authentication (ARC4, SSL-MAC-MD5/SHA-1) performance at 700 Mbps, and IPsec (3DES, HMAC-SHA-1) performance of greater than 950 Mbps. A true hardware random number generator on the BCM5825 is well-suited for Initialization Vector seeding and secret key generations.

The BCM5825 is ideal for high-end and midrange VPN and firewall appliance applications and SSL-based appliances. The BCM5825 addresses a very broad range of performance points and leverages a common software base, allowing customers to develop families of products with common architectures and software platforms.

The BCM5825 is ideal for embedded applications with strict board space and power requirements because it requires no external components. Additionally, the integrated PCI-X interface makes it a perfect solution for all high performance yet cost-sensitive security applications. In the unlikely event that more performance is required, the BCM5825 can be scaled to further increase both public-key and bulk crypto (IPsec and AES) processing performance.

System memory is optimized to maximum throughput in real-world applications with unlimited security association (SA) support via system memory and a multithreaded DMA engine. Concurrent public-key and bulk payload processing minimizes latency and improves system performance dramatically.

Application Program Interface (API) support through Broadcom's renowned Software Reference Library (SRL) for IPsec and SSL application software offers BCM5825 users a complete system solution. The BCM5825 SDK includes support for VxWorks, Linux, and BSD.

Broadcom®, the pulse logo, Connecting everything®, and the Connecting everything logo are among the trademarks of Broadcom Corporation and/or its affiliates in the United States, certain other countries and/or the EU. Any other trademarks or trade names mentioned are the property of their respective owners.

Connecting  
everything®



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

© 2006 by BROADCOM CORPORATION. All rights reserved.

5825-PB03-R 04/19/06

Phone: 949-450-8700  
Fax: 949-450-8710  
E-mail: [info@broadcom.com](mailto:info@broadcom.com)  
Web: [www.broadcom.com](http://www.broadcom.com)