Fact Sheet

MPC180

SECURITY PROCESSOR

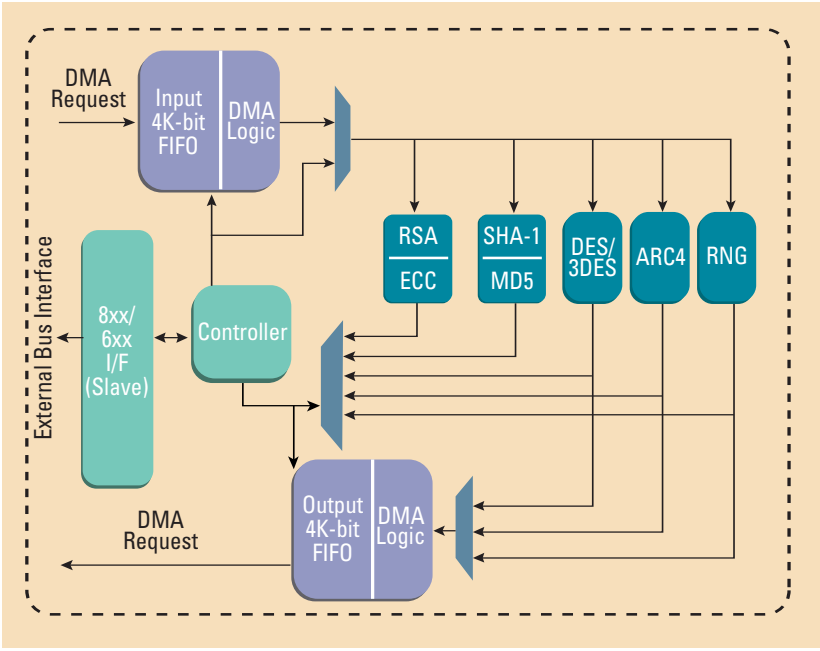
MOTOROLA intelligence everywhere™ | digital dna™

Network equipment vendors looking to integrate the latest security systems into their equipment can now turn to Motorola—the same company that makes the network and communications processors the industry knows and trusts. Derived from thirty years of security technology experience, Motorola's family of network security processors is designed to work seamlessly with Motorola's communications processors and offers an easy way to enhance the performance of network equipment without adding costly hardware.

MPC180 is a low-cost, easily integrated addition to any networking or computing system supporting Motorola's integrated communications processors. It is designed to off-load computationally intensive security functions, such as key generation and exchange, authentication, and bulk encryption from the Motorola PowerQUICC™ and PowerQUICC II™ communications processors.

The MPC180 security processor is optimized to process all the algorithms associated with IPsec, IKE, WTLS/WAP and SSL/TLS, including RSA, RSA signature, Diffie-Hellman, Elliptic Curve Cryptography, DES, 3DES, SHA-1, MD-4, MD-5, and ARC-4. The MPC180 is also able to accelerate Elliptic Curve mathematics, which is especially important for secure wireless communications.

MPC180 BLOCK DIAGRAM



MPC184 PRODUCT HIGHLIGHTS:

- Public key execution unit (PKEU), which supports the following:
  - RSA and Diffie-Hellman
  - Programmable field size 80 to 2048 bits
  - Elliptic Curve operations in either F2m or F(p)
  - Programmable field size from 55- to 511-bits
- Message authentication unit (MAU)
  - SHA-1 with 160-bit message digest
  - MD5 with 128-bit message digest
  - HMAC with either algorithm
- Data encryption standard execution units (DEUs)
  - DES and 3DES algorithm acceleration
  - Two key (K1, K2, K1) or Three key (K1, K2, K3)
  - ECB and CBC modes for both DES and 3DES
- ARC four execution unit (AFEU)
  - Implements a stream cipher compatible with the RC4 algorithm
  - 40- to 128-bit programmable key
- Random Number Generator (RNG)
- Input Buffer (4kbits)
- Output Buffer (4kbits)
- Glueless interface to MPC8xx system or MPC826x local bus (50 MHz and 66 MHz operation)
- DMA hardware handshaking signals for use with the MPC826x
- 1.8V Vdd, 3.3V I/O
- 100-pin LQFP package
- Software and development support available

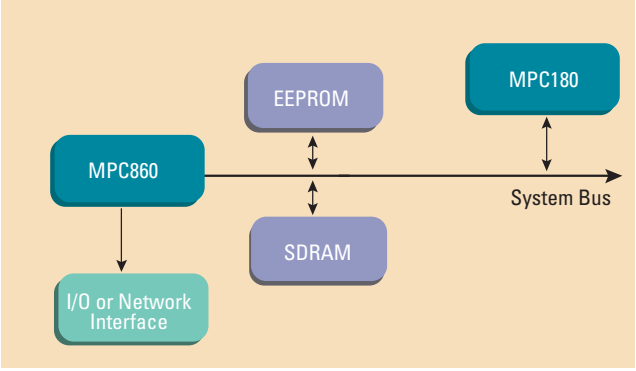
TYPICAL APPLICATIONS:

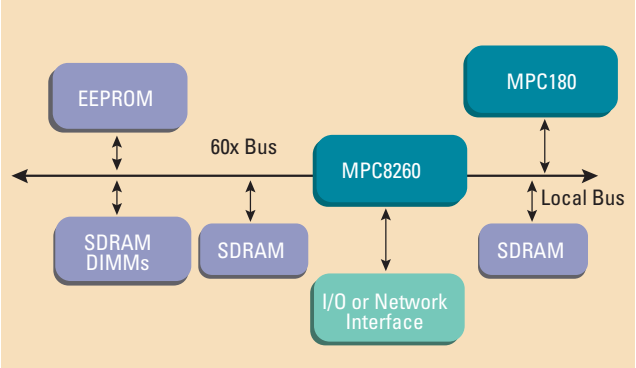
- SOHO and low-end routers
- xDSL access equipment
- ISDN access equipment
- Wireless base stations
- Broadband access
- WAP gateways
- DSLAMS
- Customer premise equipment (CPE)

MPC180 PERFORMANCE:

- 1024-bit Diffie-Hellman
  - 10 connections per second
- 155-bit ECC
  - 30 connections per second
- 3DES-HMAC-SHA-1 15.0 Mbps

MPC8XX SYSTEM EXAMPLE





MPC826X SYSTEM EXAMPLE

Bulk encryption/authentication performance estimates include data/key/context reads from memory to MPC180, writes of completed data/context back to memory assuming typical system overhead.

MOTOROLA