Advance Information

MPC180TS/D
Rev. 0.1, 2/2003

MPC180 Security Processor
Technical Summary

This document provides an overview of the MPC180 security processor, including a brief development history, target applications, key features, typical system architecture, as well as an MPC180 architectural overview.

1 Development History

The MPC180 is the first in the Smart Networks platform’s S1 family of security processors developed for the commercial networking market. It is derived from security technologies Motorola has developed over the past 30 years, primarily for government applications. The third-generation execution units (EUs) in the MPC180 have been previously used in products for wireless base stations and secure wire-line communication.

2 Typical Applications

The MPC180 is suited for applications such as the following:

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

3 Features

The MPC180 is a flexible and powerful addition to any networking system currently using Motorola’s MPC8xx or MPC826x family of PowerQUICC™ communication processors. The MPC180 is designed to off-load computationally intensive security functions such as key generation and exchange, authentication, and bulk data encryption.

The MPC180 is optimized to process all of the algorithms associated with IPSec, IKE, WTLS/WAP and SSL/TLS. In addition, the MPC180 is the only security processor on the market capable of executing the elliptic curve cryptography that is especially important for secure wireless communications.

MPC180 features include the following:

- Public key execution unit (PKEU), which supports the following:
  - RSA and Diffie-Hellman
    - Programmable field size 80- to 2048-bits
    - 1024-bit signature time of 32ms
    - 10 IKE handshakes/second
  - Elliptic Curve operations in either F 2 m or F p
    - Programmable field size from 55- to 511-bits
    - 155-bit signature time of 11ms
    - 30 IKE handshakes/second
- 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
  - 15 Mbps 3DES-HMAC-SHA-1 (memory to memory)
- Message authentication unit (MAU)
  - SHA-1 with 160-bit message digest
  - MD5 with 128-bit message digest
  - HMAC with either algorithm
- ARC four execution unit (AFEU)
  - Implements a stream cipher compatible with the RC4 algorithm
  - 40- to 128-bit programmable key
  - 20 Mbps ARC Four performance (memory to memory)
- Random Number Generator (RNG)
  - Supplies up to 160 bit strings at up to 5 Mbps data rate
- Input Buffer (4kbits)
- Output Buffer (4kbits)
- Glueless interface to MPC8xx system or MPC826x local bus (50MHz and 66MHz operation)
- DMA hardware handshaking signals for use with the MPC826x
- 1.8v Vdd, 3.3v I/O
- 100pin LQFP package
- HIP4 0.25µm process

4 Typical System Architecture

The MPC180 works well in most load/store, memory-mapped systems. An external processor may execute application code from its ROM and RAM, using RAM and optional non-volatile memory (such as EEPROM) for data storage. Figure 4-1 shows an example of the MPC180 in an MPC8xx system, and Figure 4-2 shows the MPC180 connected to the local bus of the MPC826x. In these examples, the MPC180 resides in the memory map of the processor; therefore, when an application requires cryptographic functions, it reads and writes to the appropriate memory location in the security processor.

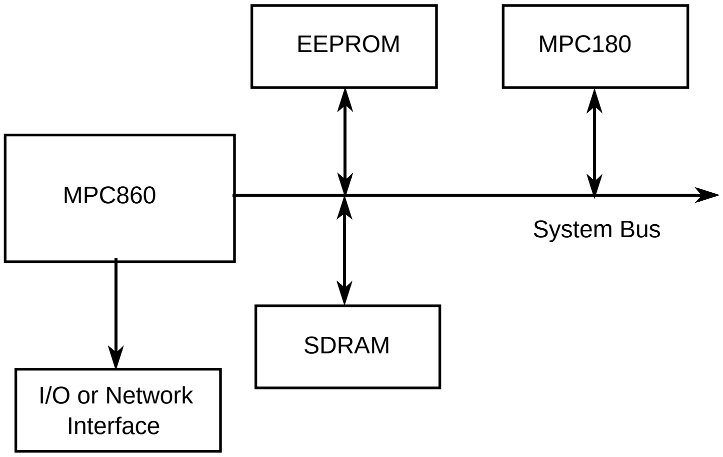

Figure 4-1. MPC8xx System Example

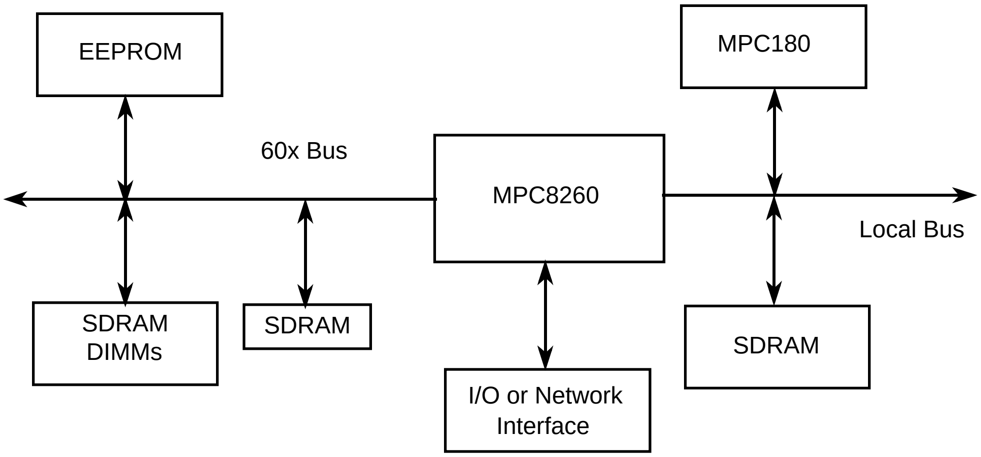

Figure 4-2. MPC826x System Example

5 Architectural Overview

The MPC180 has a slave interface to the MPC8xx system bus and MPC8260 local bus and maps into the host processor's memory space. Each encryption algorithm is mapped to a unique address space. To perform encryption operations, the host reads and writes to the MPC180 to setup the execution unit and, then, transfers data to the execution unit directly or through the external bus interface.

In FIFO mode, the MPC180 accepts data into the 4-Kbit input buffer and returns burst data through the output buffer. In this way, the host can automatically transfer bulk data through a given EU. This minimizes host management overhead and increases overall system throughput. Once the host configures the external bus interface (EBI), it receives an interrupt only after all data has been transferred or processed by the MPC180.

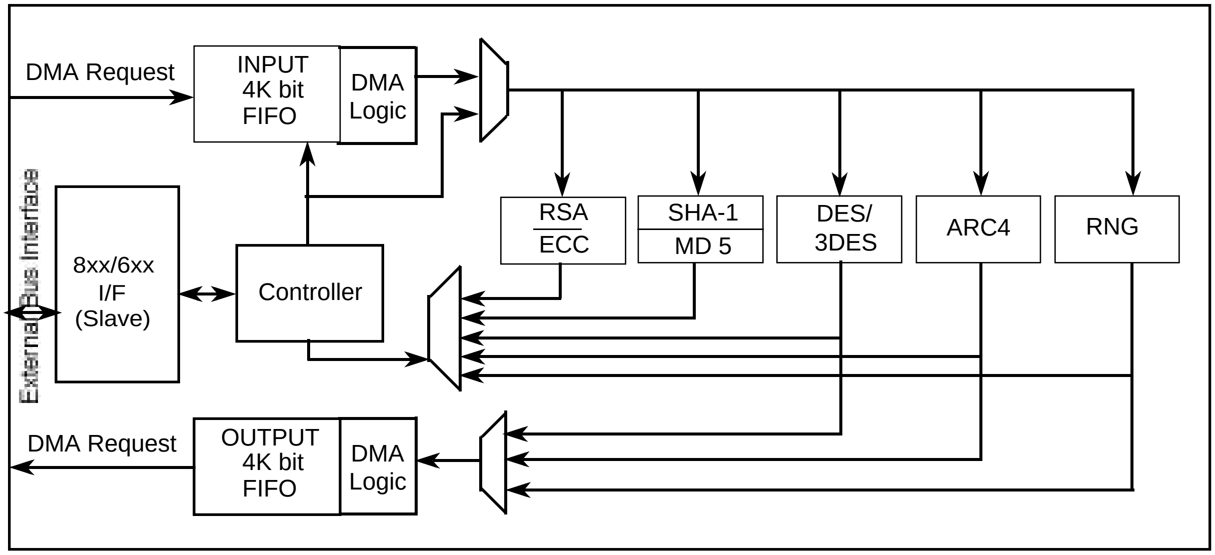

Figure 5-1. MPC180 Block Diagram

The interrupt controller organizes hardware interrupts coming from individual EUs into a single maskable interrupt, IRQ_B, for the host processor. Multiple internal interrupt sources are logically ORed to create a single, non-prioritized interrupt for the host processor. The controller lets the host read the unmasked interrupt source status as well as the request status of masked interrupt sources, thereby indicating whether a given unmasked interrupt source will generate an interrupt request to the host processor.

6 Execution Units (EU)

The execution units (EU) are the actual processing engines that implement the most common industry algorithms for cryptographic processing. The MPC180 has five execution units, each described below.

6.1 Public Key Execution Unit (PKEU)

The PKEU is capable of performing many advanced mathematical functions to support RSA and Diffie-Hellman as well as ECC in both F 2 m (polynomial-basis) and F p. The accelerator supports all levels of functions to assist the host microprocessor in performing its desired cryptographic function. For example, at the highest level, the accelerator performs modular exponentiations to support RSA and point multiplies to support ECC. At lower levels, the PKEU can perform simple operations such as modular multiplies.

6.2 Data Encryption Standard Execution Unit (DEU)

The DEU is used for bulk data encryption. It can also execute the Triple-DES algorithm, which is based on DES. The host processor supplies data to the DEU as input, and this data is encrypted and made available for reading. The session key is input to the DEU prior to encryption. The DEU computes the data encryption standard algorithm (ANSI X3.92) for bulk data encryption and decryption.

DES is a block cipher that uses a 56-bit key to encrypt 64-bit blocks of data, one block at a time. DES is a symmetric algorithm; therefore, each of the two communicating parties share the same 56-bit key. DES processing begins after this shared session key is agreed upon. The message to be encrypted (typically plain text) is partitioned into *n* sets of 64-bit blocks. Each block is processed, in turn, by the DES engine, producing *n* sets of encrypted (ciphertext) blocks. Decryption is handled in the reverse manner. The ciphertext blocks are processed one at a time by a DES module in the recipient's system. The same key is used, and the DEU manages the key processing internally so that the plaintext blocks are recovered.

The DES/3DES execution unit supports the following modes:

- ECB (electronic code book)
- CBC (cipher block chaining)

In addition to these modes, the DEU can compute Triple-DES. Triple-DES is an extension to the DES algorithm in which every 64-bit input block is processed three times. There are several ways that Triple-DES can be computed. The DES accelerator on the MPC180 supports two key (K1, K2, K1) or three key (K1, K2, K3) Triple-DES.

THe MPC180 supports two of the modes of operation defined for Triple-DES (see draft ANSI Standard X9.52-1998):

- TECB (Triple DES analogue of ECB)
- TCBC (Triple DES analogue of CBC)

6.3 ARC Four Execution Unit (AFEU)

The AFEU processes an algorithm that is compatible with the RC4 stream cipher from RSA Security, Inc. The RC4 algorithm is byte-oriented; therefore, a byte of plaintext is encrypted with a key to produce a byte of ciphertext. The key is variable length, and the AFEU supports 40-bit to 128-bit key lengths, providing a wide range of security levels. RC4 is a symmetric algorithm, so each of the two communicating parties share the same key.

AFEU processing begins after this shared session key is agreed upon. The plaintext message to be encrypted is logically partitioned into *n* sets of 8-bit blocks. In practice, the host processor groups 4 bytes at a time into 32-bit blocks and write that data to the AFEU. The AFEU internally processes each word one byte at a time. The AFEU engine processes each block in turn, byte by byte, producing *n* sets of encrypted (ciphertext) blocks. Decryption is handled in the reverse manner. The ciphertext blocks are processed one at a time by an AFEU in the recipient's system. The same key is used, and the AFEU manages the key processing internally so that the plaintext blocks are recovered.

The AFEU accepts data in 32-bit words per write cycle and produces 4 bytes of ciphertext for every 4 bytes of plaintext. Before any processing occurs, the key data is written to the AFEU, after which an initial permutation on the key happens internally. After the initial permutation is finished, processing on 32-bit words can begin.

6.4 Message Authentication Unit (MAU)

The MAU can perform SHA-1, MD5 and MD4, three of the most popular public message digest algorithms. At its simplest, the MAU receives 16 32-bit registers containing a message, and produces a hashed message of 128 bits for MD4/MD5 and 160 bits for SHA-1. The MAU also includes circuitry to automate the process of generating an HMAC (hashed message authentication code) as specified by RFC 2104. The HMAC can be built upon any of the hash functions supported by MAU.

6.5 Random Number Generator (RNG)

Because many cryptographic algorithms use random numbers as a source for generating a secret value, it is desirable to have a private RNG for use by the MPC180. The anonymity of each random number must be maintained, as well as the unpredictability of the next random number. The private RNG allows the system to develop random challenges or random secret keys. The secret key can thus remain hidden from even the high-level application code, providing an added measure of physical security. The RNG is also useful for digital signature generation.

The RNG is a digital integrated circuit capable of generating 32-bit random numbers. It is designed to comply with FIPS-140 standards for randomness and non-determinism. The RNG creates an unpredictable sequence of bits and assembles a string of those bits into a register. The random number in that register is accessible to the host through the host interface of the RNG.

7 Software and Hardware Support

Customers will have access to device drivers integrated with the WindRiver VxWorks OS. Sample drivers will also be provided to customers wishing to integrate MPC180 support into other operating systems.

Third-party support for the MPC180 includes a development system for both the MPC860 and the MPC8260. The WindRiver/EST SBC8260C development system and Zephyr Engineering ZPC860C, both of which include a board support package, are available to accelerate customer design cycles.

8 Revision History

Table 8-1 summarizes the revision history of this document.

Table 8-1. Revision History

Revision No.	Substantive Change(s)
0	Initial release.
0.1	Added revision history and updated with new template.

THIS PAGE INTENTIONALLY LEFT BLANK

HOW TO REACH US:

USA/EUROPE/LOCATIONS NOT LISTED:

Motorola Literature Distribution
P.O. Box 5405, Denver, Colorado 80217
1-303-675-2140
(800) 441-2447

JAPAN:

Motorola Japan Ltd.
SPS, Technical Information Center
3-20-1, Minami-Azabu Minato-ku
Tokyo 106-8573 Japan
81-3-3440-3569

ASIA/PACIFIC:

Motorola Semiconductors H.K. Ltd.
Silicon Harbour Centre, 2 Dai King Street
Tai Po Industrial Estate, Tai Po, N.T., Hong Kong
852-26668334

TECHNICAL INFORMATION CENTER:

(800) 521-6274

HOME PAGE:

www.motorola.com/semiconductors

Information in this document is provided solely to enable system and software implementers to use Motorola products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits or integrated circuits based on the information in this document.

Motorola reserves the right to make changes without further notice to any products herein. Motorola makes no warranty, representation or guarantee regarding the suitability of its products for any particular purpose, nor does Motorola assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. “Typical” parameters which may be provided in Motorola data sheets and/or specifications can and do vary in different applications and actual performance may vary over time. All operating parameters, including “Typicals” must be validated for each customer application by customer’s technical experts. Motorola does not convey any license under its patent rights nor the rights of others. Motorola products are not designed, intended, or authorized for use as components in systems intended for surgical implant into the body, or other applications intended to support or sustain life, or for any other application in which the failure of the Motorola product could create a situation where personal injury or death may occur. Should Buyer purchase or use Motorola products for any such unintended or unauthorized application, Buyer shall indemnify and hold Motorola and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, and expenses, and reasonable attorney fees arising out of, directly or indirectly, any claim of personal injury or death associated with such unintended or unauthorized use, even if such claim alleges that Motorola was negligent regarding the design or manufacture of the part.