



MosChip Security Processor MCS1000

Frequently Asked Questions

Version 2.0

February 20, 2004

For more information contact the Technical Marketing Group:

info@moschip.com (408) 737-7141 x124

www.moschip.com

All information in this document is believed to be accurate as of the publish date.

VPN^{Now}™ is a registered trademark of Artec Group. ARM is a registered trademark of ARM Limited. All other brands or product names are the property of their respective holders.

MosChip Semiconductor products are not authorized for use as critical components in life support devices or systems without the express written approval of the president of MosChip Semiconductor, Ltd.

MosChip Semiconductor believes the information in this document to be accurate and reliable. However, it is subject to change without notice. No responsibility is assumed by MosChip Semiconductor for its use, nor for infringement of patent or other rights of third parties. No part of this document may be reproduced, or transmitted in any form or by any means without prior consent of MosChip Semiconductor, Ltd.

Copyright © 2004 MosChip Semiconductor All Rights Reserved.

Hardware

Q: What processor core is used in the MCS1000?

A: ARM926EJ-S, 32-bit CPU. See www.arm.com for details on the ARM core.

Q: What cryptographic standards are supported?

A: Encapsulating Security Payload: DES, 3DES, and AES;
Authentication Headers: SHA, and MD5

Q: Does the MCS1000 support SSL?

A: No. SSL uses RC2 and RC4 encryption from RSA. SSL is not purely packet-based and requires links higher into the stack so it cannot be transparent to the system.

Q: At what geometry is the MCS1000 fabricated?

A: 0.18u

Q: What supply Voltages are required?

A: 1.8 Volts for the core and 3.3 Volts for the I/O

Q: Is Flash and SDRAM required to run the MCS1000?

A: SDRAM is always required for code execution and storage of the Policy and Security Association Data Bases. When used in peripheral mode Flash is not required because code can be loaded via the PCI interface from the host. Flash is required for code storage when the MCS1000 is used in standalone mode.

Q: Can the MAC address be placed in Flash?

A: There is an interface for an external EEPROM, but the MAC address can also be programmed onto an external Flash if one is present.

Q: What type of EEPROM should be used?

A: Either an SPI or an I2C EEPROM can be used. See the MCS1000 Development Board schematic for details.

Q: Is the PHY and the MAC in the MCS1000?

A: Yes. All three (3) Ethernet ports of the MCS1000 can be connected directly to magnetics. There is also a provision to connect Ethernet port A to an optical transceiver.

Q: Can an MII on an Ethernet port be accessed.

A: Yes. There is an alternate PHY configuration where two PHYs are used and one MII is available. In this mode some GPIO, LED, and serial port signals are lost.

Q: What is the maximum speed of the serial port?

A: 115,200Baud

Q: Can the MCS1000 be the host in a PCI-based system?

A: Yes and no. The MCS1000 does not have an arbiter. It can only be a device in a large PCI system, but if only one device is used, then the MCS1000 can master the PCI bus. An example would be a need for a single 802.11 interface. In this case a single additional device can be added via the PCI/CardBus interface.

Q: What is the speed and width of the PCI interface?

A: The PCI interface is a 32-bit 33MHz interface. It complies with the PCI 2.2 standard.

Q: What is the speed of Local Bus?

A: The Local bus is a 32-bit 50 MHz bus.

Q: Does the MCS1000 have a Memory Management Unit (MMU) in order to use Linux?

A: Yes. The ARM926EJ-S has an MMU will run Linux, VxWorks, MQX, and other RTOSs.

Q: What are the sizes of the caches?

A: There is a 32KB data cache, a 32KB instruction cache, and a 16KB packet cache.

Q: What is the data width of the Flash interface?

A: 8-bit, 16-bit, or 32-bit

Q: What is the maximum amount of flash?

A: There are 26 bits of addressing so:

8-bit = 64Mbytes

16-bit = 128Mbytes

32-bit = 256Mbytes

Q: What types of SDRAM are supported?

A: 100MHz SDRAM. DDR and QDR are not supported.

Q: Can 133 or 166MHz SDRAM be used?

A: Yes.

Q: What is the maximum amount of SDRAM supported by the MCS1000?

A: 64 Mega bytes

Q: What is the SDRAM data-bus width?

A: 32 bits

Software

Q: What Operating Systems (OS) are supported by the MCS1000?

A: Since the MCS1000 is based on the popular ARM9 core there are many OSES which can be used with the MCS1000.

Q: What does MosChip offer in the way of OS support?

A: MosChip ported a version of the Linux OS kernel 2.4.18 along with the FreeS/WAN application which has been modified to operate with the VPNNow™ Hardware Module .

Development Board

Q: What software is included with the MCS1000 Development Board?

A: MosChip provides a booting Linux kernel, FreeS/WAN, GNU tools, ARM boot code, software libraries, and other code for rapid development of VPN applications.

Q: What type of emulation tools are available?

A: ARM has a JTAG-based ICE (Multi-ICE® Interface Unit p/n MI220-KT-0175A)
http://www.arm.com/devtools/multi_ice?OpenDocument

Q: Do I need to buy ARM development tools in order to work with the MCS1000?

A: If the developer would like to design their own software, then the ARM Developer Suite p/n DS120-KT-40000 or -30000 may be required for custom software development.
<http://www.arm.com/devtools/ADS?OpenDocument>

However, most projects can use the Linux software provided by MosChip (GNU tools) along with standard software packages such as BOOTP and TFTP for software development.

Q: In what formats are the reference designs available?

A: Bill of Materials is in Excel, Schematics are in OrCad and the lay-out is in PADS.

System Issues

Q: I would like to use the MCS1000 in peripheral mode as a secure Ethernet NIC. What drivers are available?

A: MosChip will provide Windows and Linux drivers in order to use the MCS1000 in peripheral mode.

Q: How do I integrate my existing IKE system with the MCS1000?

A: An API is provided that details how the data is exchanged between applications and the MCS1000.

Q: Does the MCS1000 support IPV6?

A: The MCS1000 supports Ethernet transactions under the current Ethernet standard (IP version 4) as well as the new Ethernet standard (IP version 6) with the extended addressing octets.

Q: Does the MCS1000 do Network Address Translation and Traversal (NAT) or Port and Packet Filtering?

A: Yes. The MCS1000 can perform most higher-layer protocols, but those protocols need to be implemented in the OS or by custom software.

Q: What types of Internet Key Exchange does the MCS1000 support?

A: IKE is implemented on the host system when the MCS1000 is used in peripheral mode and the MCS1000 implements the IKE when in standalone mode. The IKE is performed by developer defined software whether on the MCS1000 or the host so the IKE methods are only constrained by the developer defined software.

Availability

Q: When will MCS1000 samples and development systems be available?

A: Development systems and sample chips are available now.

Q: When will production quantities of the MCS1000 be available?

A: Q2 of 2004

Q: I need a full datasheet. Is one available?

A: The full hardware manual and software manual along with other documentation are available on the MosChip Website www.moschip.com.