VMS115

Application Note

External Processor Interface

Revision: 1.0

Table of Contents

1.0 Introduction

1.1 Purpose

This Application Note describes how the VMS115 interfaces to an external processor. Descriptions of physical connections as well as the programming interface are explained.

1.2 References

[1] VMS115 Data Sheet (see http://www.vlsi.com/library/ad_bul.shtml for the latest version)

[2] FIPS 140-1, Security Requirements for Cryptographic Modules, January 11, 1994, National Institute of Standards and Technology (http://csrc.nist.gov)

[3] FIPS 46-2, Data Encryption Standard, National Institute of Standards and Technology (http://csrc.nist.gov)

[4] FIPS 81, Modes of Operation of the DES, National Institute of Standards and Technology (http://csrc.nist.gov)

[5] FIPS 186, Digital Signature Standard, May 19, 1994, National Institute of Standards and Technology (http://csrc.nist.gov)

[6] FIPS 180-1, Secure Hash Standard, April 17, 1995, National Institute of Standards and Technology (http://csrc.nist.gov)

Definitions and Acronyms

DES .....Data Encryption Standard

DES CBC.....DES Cipher Block Chaining

DES ECB .....DES Electronic Code Book

DSTL .....Dual State Transition Logic

DRAM .....Dynamic Random Access Memory

HMAC.....Hash Message Authentication Code

IPSec .....Internet Protocol Security

Mbps .....Megabits per second

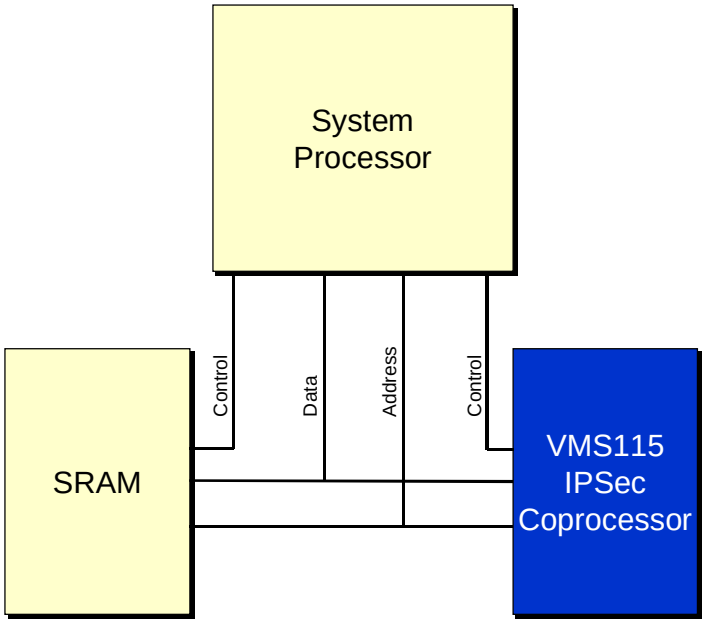
MD5 .....Message Digest, Version 5

SHA-1 .....Secure Hashing Algorithm, Version 1

SRAM .....Scratch Random Access Memory

2.0 Physical Connections

The VMS115 IPSec Coprocessor is well suited for the following system configuration. The VMS115 is designed to communicate with an external processor just as the processor would communicate with an external SRAM.



2.1 System Connection

This section explains how the VMS115 could connect to a system processor without any DMA functionality. If there is DMA functionality available, then the VMS115's ORDY and IRDY lines would be connected to the system processor's DMA signals.

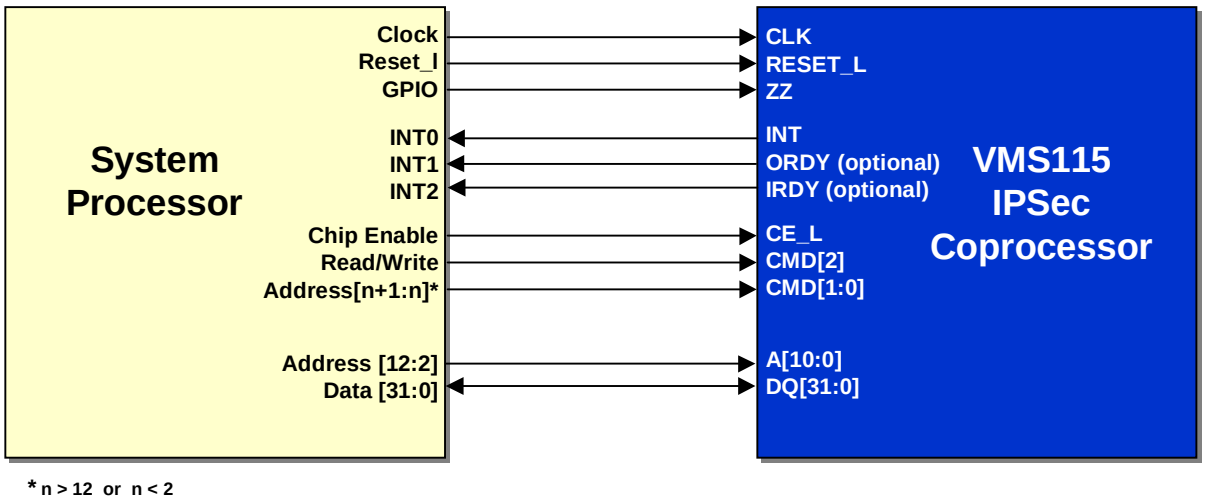


Table 2-1: System Setup Connection Description

VMS115		System Processor		
Pin	**I/O**	**I/O**	**Pin**	**Description**
CLK	Input	Output	Clock	System Clock output to VMS115 and external memory.
RESET_L	Input	Output	Reset_l	External reset output signal.
ZZ	Input	Output	GPIO	If using the VMS115 Sleep Mode a GPIO output signal may be used to drive the VMS115 ZZ signal.
INT	Output	Input	INT0	A single interrupt input from the VMS115 may be used instead of using both the ORDY and IRDY signals. If using a single INT line, then the Interrupt Status Register must be read to determine the source of the interrupt.
ORDY	Output	Input	INT1	If enough interrupt pins are available, the ORDY and IRDY signals may drive separate interrupts. This will eliminate the need to read the Interrupt Status Register to determine the interrupt source.
IRDY	Output	Input	INT2	
CE_L	Input	Output	Chip Enable	Chip Enable output to the VMS115.
CMD[2]	Input	Output	Read/Write	Read/Write output to CMD[2]. The high order bit determines if the command is a VMS115 read or write operation.
CMD[1:0]	Input	Output	Address Lines	Address lines may be used to complete the command to the VMS115. The final two bits of the command determine what type of memory is being read from or written to the VMS115 (register space, packet data or context).
A[10:0]	Input	Output	Address[12:2]	The VMS115 is a word addressable device. The system processor should connect it's address lines to the VMS115 beginning with Address line 2 connecting to the VMS115's Address line 0, Address 3 to VMS115 Address 1 and so on. See Address Line Connections (see section 2.2).
DQ[31:0]	I/O	I/O	Data[31:0]	Data lines are connected directly to the VMS115 data lines.
TDI	Input	Output	Ground	The TDI input should be driven low.
TDO	Output	Input	Open	The TDO output should be open.
TMS	Input	Output	Ground	The TMS input should be driven low.

2.2 Address Line Connections

The following table describes how the VMS115 Address lines are intended to be connected with an external processor. The address map in the VMS115 Data Sheet describes the address expected on the VMS115 address lines.

The following example is accessing the VMS115 Configuration Register at location 0x402.

VMS115	Hex Value	4			0				2				
	Address	A[10]	A[9]	A[8]	A[7]	A[6]	A[5]	A[4]	A[3]	A[2]	A[1]	A[0]	x	x
Data		1	0	0	0	0	0	0	0	0	1	0	0	0
Processor	Address	A[12]	A[11]	A[10]	A[9]	A[8]	A[7]	A[6]	A[5]	A[4]	A[3]	A[2]	A[1]	A[0]
	Hex Value	1	0				0				8			