



Product Type            Integrated Communication Processor

Freescale Part #        MPC185VF

Name                     Talos

Package                  256 MAP BGA

Algorithms		Max Key Size (bits)
	DES (ECB, CBC)	56
	3DES (ECB, CBC)	168 (3-keys)
	AES (ECB, CBC, CTR, CCM)	256
	ARC-4	128
	MD-5+ HMAC	(up to 512 bit keys)
	SHA-1+ HMAC	(up to 512 bit keys)
	SHA-256+ HMAC	(up to 512 bit keys)
	RSA Digital Signature	2048-bit operands
	RSA Digital Verify	2048-bit operands
	ECC Digital Signature	512-bit field or modulus size
	ECC Digital Verify	512-bit field or modulus size
	RNG	On chip 32-bit

Target Applications     :  
eCommerce servers, DSLAMs, Broadband Gateways, high end routers, 3G base stations

Export Control Info:  
ENC Status: Restricted. US EAR part 740.17(b)(2)  
ECCN: 5A002  
CCAT: G026024

#### Overview:

The MPC185 is a memory-mapped device designed to interface to the 60x bus of processors implementing the PowerPC architecture. The MPC185 is capable of acting as a bus master, or as a bus slave. With the MPC185 in slave mode, an application being executed on a host processor can accelerate cryptographic functions by writing instructions, keys, and data to the MPC185, and reading the result. Alternately, the MPC185 can act as a bus master. In this mode, the host processor determines which cryptographic function needs to be performed on a block of data, and creates a descriptor (in system memory) which describes the function to perform, and the location of the data in memory. The host writes a pointer to the descriptor directly to the MPC185, and the MPC185 fetches all additional instructions and data required to complete a high level cryptographic function. Upon completion of processing, the MPC185 writes the permuted data back to memory. The MPC185 is expected to achieve 200+ public key exchanges per second, and ~500Mbps 3DES throughput.