Product Type	Digital Signal Processor
Freescale Part #	MSC8156E
Package	783 pin 29x29 1mm pitch FC PBGA

Algorithms	**Max Key Size (bits)**
DES (ECB, CBC, OFB, CFB)	56
3DES (ECB, CBC, OFB, CFB)	168 (3-keys)
AES (ECB, CBC, CTR, CCM, CMAC, GCM, OFB, CFB, XCBC-MAC)	256
ARC-4	128
MD-5 + HMAC	(up to 512 bit keys)
SHA-1 + HMAC	(up to 512 bit keys)
SHA-224 + HMAC	(up to 512 bit keys)
SHA-256 + HMAC	(up to 512 bit keys)
SHA-384 + HMAC	(up to 512 bit keys)
SHA-512 + HMAC	(up to 512 bit keys)
Kasumi (A5/3, GEA-3, f8, f9)	128
Snow 3G	128
RSA Digital Signature	4096-bit operands
RSA Digital Verify	4096-bit operands
ECC Digital Signature	1023-bit field or modulus size
ECC Digital Verify	1023-bit field or modulus size
FIPS compliant deterministic RNG	On chip 32-bit

Target Applications :
Wireless base stations, telecom equipment

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

Overview:
The MSC8156E is a member of the StarCore^{TM} multi-core digital signal processors family from Freescale Semiconductor. The MSC8156E processor is a six-core device based on SC3850 StarCore DSP core technology and designed to dramatically advance the capabilities of wireless broadband base station equipment. The MSC8156E includes an on-chip encryption acceleration unit which is derived from the MPC185, a Freescale Encryption Co-Processor already granted ENC status (CCAT: G026024). This on-chip encryption accelerator (also known as the SEC 3.1) is expected to achieve ~1000 Mbps AES-128 throughput.

The SEC 3.1 supports the following enhancements compared to the MPC185.
DES/3DES – adds OFB and CFB modes
AES – adds CMAC, GCM, OFB, CFB, XCBC-MAC, and XTS modes
Snow3G – as recommended by ETSI for 3G security
Hashing – adds support for SHA-224, SHA-384, and SHA-512
Public Key – extends RSA operand length to 4096b (from 2048b), and Elliptic Curve operand length to 1023b (from 511b)