



Product Type Integrated Communication Processor
 Freescale Part # MPC8572E, MPC8571E
 Name PowerQUICC 38H
 Package 1023 FC PBGA
 Crypto Hardware SEC 3.0

<u>Algorithms</u>	<u>Max Key Size (bits)</u>
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
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:

Access routers, wireless access points, wireless base stations, telecom equipment, storage controllers

Export Control Info:

Harmonized Tariff (US): 8542.31.0000
 ENC Status: Restricted. US EAR part 740.17(b)(2)
 ECCN: 5A002
 CCAT: G026024

Overview:

The MPC8572E and MPC8571E are members of the PowerQUICC 3 family of integrated communications processor from Freescale Semiconductor. The PowerQUICC 3 is considered one of the most highly integrated and widely adopted communications processor in the world, and is capable of supporting most LAN and WAN networking standards. MPC8572E/8571E family 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 3.0) is expected to achieve 1000+ public key exchanges per second, and ~2000 Mbps 3DES throughput.

The SEC 3.0 supports the following enhancements compared to the MPC185.

- DES/3DES – adds OFB and CFB modes
- AES – adds CMAC, GCM, OFB, CFB, XCBC-MAC modes
- 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)