| | |
|---|---|
| Product Type | Integrated Communication Processor |
| Freescale Part # | P1010, P1014 |
| Package | 425 pin 19x19mm TePBGA-I |
| Crypto Hardware | SEC 4.4 |

| **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 LAN Access Points, SMB Routers

Export Control Info:
Harmonized Tariff (US): 8542.31.0000
ENC Status: Restricted. US EAR part 740.17(b)(2)
ECCN: 5A002
CCAT: G068311

Overview:
The P1010 and P1014 are members of the QorIQ family of integrated communications processor from Freescale Semiconductor. The P1010 incorporates a 32b e500 Power Architecture CPU cores, 1 DDR3 Memory Controller, 3 -1G ethernet controllers, and USB, SATA, and CAM peripheral bus controllers. The P1010 also provides support for secure boot and platform assurance.

The P1014 has one less Ethernet controller , no CAN, a narrower DDR interface, and does not support the QorIQ Platform's Trust Architecture, but otherwise has the same features as the P1023.

The P1010 and P1014 also integrate a 2Gbps Crypto Acceleration Engine (SEC 4.4). The algorithms and key lengths supported by the SEC 4.4 are listed in the table above.

In addition to crypto algorithm processing, the SEC 4.4 supports security protocol processing off-load capability, with specific support for protocol header and trailer processing for IPsec, SSL, DTLS, SRTP, MACSec, 802.16e, and 802.11e. The SEC 4.2 is expected to achieve 5000+ public key exchanges per second.