| | |
|---|---|
| Product Type | Integrated Communication Processor |
| Freescale Part # | LS1043A, LS1023A |
| Package | 23x23 780 FC PBGA, 21x21 621 FC PBGA |
| Crypto Hardware | SEC 5.4 |

| **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 |
| 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 |
| ZUC (EEA-1 & EIA-2) | 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 :
Control processing for Routers, Storage Arrays, Industrial Single Board Computers

Export Control Info:
Harmonized Tariff (US): 8542.31.0000
ENC Status: Restricted. US EAR part 740.17(b)(2)
ECCN: 5A002A.1
CCAT: G161023

Overview:
The LS1043A and LS1023A are members of the QorIQ family of integrated communications processor from Freescale Semiconductor.

The LS1043A incorporates (4) 64b A53 ARM Architecture CPU cores, (1) DDR3L/4 Memory Controller, (5) 1G Ethernet ports and (1) 10 Ethernet port, along with multiple PCIe, SATA, and USB peripheral bus controllers.

The LS1023A incorporates (2) 64b A53 ARM Architecture CPU cores, (1) DDR3L/4 Memory Controller, (5) 1G Ethernet ports and (1) 10 Ethernet port, along with multiple PCIe, SATA, and USB peripheral bus controllers.

In addition to these CPUs and interfaces, the LS1043A and LS1023A integrate a 7Gbps Crypto Acceleration Engine (SEC 5.4). The algorithms and key lengths supported by the SEC 5.4 are listed in the table above.

In addition to crypto algorithm processing, the SEC 5.4 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 5.4 is expected to achieve 2500+ public key exchanges per second.

The LS1043A and LS1023A also provide support for secure boot and platform assurance and ARM TrustZone.

NOTE 1: This authorization does not authorize the export of products designed to use the encryption functionality of these chips. Such products may require a classification and/or license from the Bureau of Industry and Security (BIS) prior to export. OEMs incorporating these chips in their products should call the BIS Encryption Export Support Line at 202-482-0707 with specific questions.

NOTE 2: Freescale Semiconductor ("Freescale") makes this export classification and regulatory information available for informational purposes only. It may not reflect the most current legal developments, and Freescale does not represent, warrant or guarantee that it is complete, accurate or up-to-date. This information is subject to change without notice. The contents of this fact sheet are not intended to constitute legal advice or to be used as a substitute for specific legal advice from a licensed attorney and or customs broker. You should not act or refrain from acting based upon information in this email without obtaining professional advice regarding your particular facts and circumstances.