Product Type	Integrated Communication Processor
NXP Part #	LS1028A, LS1018A, LS1027A, LS1017A
Package	17mm x 17mm, 448 flip-chip plastic ball grid array (FC-PBGA)
Crypto Hardware	SEC 5

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 :
Combined control, datapath, and application layer processing in Industrial & IoT Gateways, Wireless LAN (WLAN) Access Point, Industrial HMI, Programmable Logic Controller (PLC), Motion Control and Robotics
.

Export Control Info:
Harmonized Tariff (US): 8542.31.0000
ENC Status: Restricted. US EAR part 740.17(A) and 740.17(B)(2)(i)(A)
ECCN: 5A002A.1
CCAT: G175850

Overview:
The LS1028A, LS1018A, LS1027A, and LS1017A are members of the QorIQ Layerscape family of integrated communications processors from NXP Semiconductor.

The LS1028A & LS1027 incorporate (2) 64b A72 ARM Architecture CPU cores, (1) 16-32b DDR3L/4 Memory Controllers, multiple high speed (1, 2.5G) Ethernet controllers, along with multiple PCIe and other peripheral bus controllers. The

LS1018A & LS1017 incorporate (1) 64b A72 ARM Architecture CPU core, but are otherwise the same as LS1028A & LS1027A.

The LS1028A and LS1018A incorporate a 3D GPU, LCD controller, and DisplayPort interface, which is not found in the LS1027A and LS1017A.

In addition to these CPUs and interfaces, the LS1028/27/18/17 family integrates a ~5Gbps Crypto Acceleration Engine (SEC 5). The algorithms and key lengths supported by the SEC 5 are listed in the table above.

The SEC 5 also 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 is expected to achieve 1500+ public key operations per second.

The LS1028/27/18/17 family also provides support for secure boot and platform assurance, including 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: NXP Semiconductor ("NXP") makes this export classification and regulatory information available for informational purposes only. It may not reflect the most current legal developments, and NXP 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.