Product Type	Integrated Communication Processor
Freescale Part #	C291, C292, C293
Name	CoIQ
Package	780 FC-PBGA

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)
RSA Digital Signature	4096-bit operands
RSA Digital Verify	4096-bit operands
ECC Digital Signature	1024-bit field or modulus size
ECC Digital Verify	1024-bit field or modulus size
FIPS compliant deterministic RNG	On chip 32-bit

Target Applications :
eCommerce servers, Hardware Security Modules, Network Admission Control appliances, VPN routers and Security Appliances, Application Delivery Controllers

Export Control Info:
Harmonized Tariff (US): 8542.31.0000
ENC Status: Restricted. US EAR part 740.17(b)(2)
ECCN: 5A002.A.1
CCAT: G150223

Overview:

The C29x family consists of 3 family members; the C291, C292, and C293. All devices are pin compatible. C29x products are optimized for public key operations. Public key algorithms such as RSA, Diffie Hellman, and Elliptic Curve Cryptography (ECC) are the basis of digital signature and key exchange protocols that make electronic commerce possible.

C29x products can be used as cryptographic co-processors, off-loading public key operations from a host CPU. When operating in this mode, the C29x connects to the host via PCIe, with the C29x requiring no external memory; neither NVRAM nor DDR, and generally no peripheral ICs. The host handles packet Rx & Tx functions, classification, protocol termination, etc, and defines the operations it wants the C29x to perform via descriptors. In addition to performing cryptographic acceleration using keys managed by the external host, the C29x can also use keys that are protected even from the host. This use case leverages the Trust Architecture, first introduced in the Freescale QorIQ communication processor family. The Trust Architecture gives the C29x secure boot and secure storage capability, insuring that factory loaded keys can only be decrypted and used by the C29x when the C29x is executing trusted software.

The C291 is targeted to achieve ~8000 2048b RSA operations per second, the C292 ~17,000, and the C293 ~31,000.

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.