



Product Type	Integrated Communication Processor
Freescale Part #	P2040, P2041
Package	783 FC PBGA
Crypto Hardware	SEC 4.2

**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 :  
Enterprise Routers, Switch Controllers, Wireless Base Stations, Industrial Single Board Computers

Export Control Info:  
Harmonized Tariff (US): 8542.31.0000  
ENC Status: Restricted. US EAR part 740.17(b)(2)  
ECCN: 5A002 A.1  
CCAT: G144297

Overview:  
The P2040 and P2041 are members of the QorIQ family of integrated communications processor from Freescale Semiconductor. The P2040 and P2041 incorporate 4x 32b e500 Power Architecture CPU cores, 1 DDR3/3L Memory Controller, and 5x 1G Ethernet Controllers (and one XAUI controller for P2041), along with multiple PCIe and sRIO peripheral bus controllers. In addition to these CPUs and interfaces, the P2040 and P2040 integrate a 5Gbps Pattern Matching Engine (regex), and a 5Gbps Crypto Acceleration Engine (SEC 4.2). The algorithms and key lengths supported by the SEC 4.2 are listed in the table above.



In addition to crypto algorithm processing, the SEC 4.2 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.

The P2040 and P2041 also provide support for secure boot and platform assurance.

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.



**UNITED STATES DEPARTMENT OF COMMERCE  
BUREAU OF INDUSTRY AND SECURITY  
WASHINGTON, D.C. 20230**

CASE NUMBER: Z411731

FREESCALE SEMICONDUCTOR, INC.  
ATTN: Herika Baker  
6501 WILLIAM CANNON DRIVE WEST  
AUSTIN, TX 78660

June 8, 2012  
G144297

BIS ISSUES THIS COMMODITY CLASSIFICATION DETERMINATION BASED UPON THE ASSUMPTION THAT THE APPLICANT HAS ALREADY DETERMINED THAT THE ABOVE-LISTED ITEM(S) ARE "SUBJECT TO THE EAR". AS DEFINED AND DESCRIBED IN SECTIONS 734.2 THROUGH 734.4 OF THE EAR, THE TERM "SUBJECT TO THE EAR" MEANS, AMONG OTHER THINGS, THAT THE ITEM(S) ARE NOT EXCLUSIVELY CONTROLLED FOR EXPORT OR REEXPORT BY ANOTHER AGENCY OF THE U.S. GOVERNMENT. SEE 15 C.F.R. 734.3(B)(1). THIS COMMODITY CLASSIFICATION DETERMINATION IS NOT A DETERMINATION BY BIS AS TO WHETHER THE ABOVE-LISTED ITEMS ARE "SUBJECT TO THE EAR". THUS, THIS DOCUMENT IS NOT AND MAY NOT BE RELIED UPON AS A U.S. GOVERNMENT DETERMINATION THAT THE ABOVE-LISTED ITEMS ARE NOT, FOR EXAMPLE, SUBJECT TO THE EXPORT CONTROL JURISDICTION OF THE INTERNATIONAL TRAFFIC IN ARMS REGULATIONS (ITAR) (22 C.F.R. PARTS 120-130), WHICH ARE ADMINISTERED BY THE U.S. DEPARTMENT OF STATE.

THE FOLLOWING INFORMATION IS IN RESPONSE TO YOUR INQUIRY OF May 17, 2012 REQUESTING LICENSE INFORMATION FOR:

COMMODITY	ECCN	LVS	IVL REQUIRED LVS DOLLAR LIMIT FOR COUNTRY GROUP
P2010 and P2020 - QorIQ P2 family of communications processors. P2010_P2020	5A002a.1		\$
P2040 and P2041 - QorIQ P2 family of communications processors. P2040_P2041	5A002a.1		\$

COMMENTS FROM LICENSING OFFICER(S) :

ITEM #1:

THIS ENCRYPTION ITEM IS AUTHORIZED FOR LICENSE EXCEPTION ENC UNDER SECTIONS 740.17 (A) AND (B) (2) OF THE EXPORT ADMINISTRATION REGULATIONS. FOR ITEMS AUTHORIZED UNDER 740.17(B) (2), THE EAR MAY REQUIRE SUBMISSION OF A SEMI-ANNUAL REPORT IN ACCORDANCE TO 740.17(E).

ITEM #2:



UNITED STATES DEPARTMENT OF COMMERCE  
BUREAU OF INDUSTRY AND SECURITY  
WASHINGTON, D.C. 20230

THIS ENCRYPTION ITEM IS AUTHORIZED FOR LICENSE EXCEPTION ENC UNDER SECTIONS 740.17 (A) AND (B) (2) OF THE EXPORT ADMINISTRATION REGULATIONS. FOR ITEMS AUTHORIZED UNDER 740.17(B) (2), THE EAR MAY REQUIRE SUBMISSION OF A SEMI-ANNUAL REPORT IN ACCORDANCE TO 740.17(E).

ITEMS OTHERWISE ELIGIBLE FOR EXPORT OR REEXPORT UNDER A LICENSE EXCEPTION OR NLR (NO LICENSE REQUIRED) AND USED IN THE DESIGN, DEVELOPMENT, PRODUCTION OR USE OF NUCLEAR, CHEMICAL OR BIOLOGICAL WEAPONS OR MISSILES REQUIRE A LICENSE FOR EXPORT OR REEXPORT AS PROVIDED IN PART 744 OF THE EXPORT ADMINISTRATION REGULATIONS (EAR).

DESTINATIONS REQUIRING A LICENSE

SEE THE COMMERCE COUNTRY CHART (SUPPLEMENT NO. 1 TO PART 738 OF THE EAR) TO DETERMINE WHICH COUNTRIES REQUIRE A LICENSE. USE THE COUNTRY CHART COLUMN INFORMATION GIVEN ON THIS FORM IN CONJUNCTION WITH THE COUNTRY CHART TO DETERMINE THE LICENSING REQUIREMENTS FOR YOUR PARTICULAR ITEMS. FOR ITEMS CLASSIFIED EAR99, SEE PART 746 OF THE EAR TO DETERMINE THE LICENSING REQUIREMENTS.

APPLICATIONS FOR EXPORT MUST BE SUBMITTED ON FORM BIS-748P MULTIPURPOSE APPLICATION. THESE FORMS MAY BE OBTAINED BY CALLING (202) 482-3332 OR REQUESTING DIRECTLY ON THE BIS INTERNET WEB SITE. ASSISTANCE IN FILLING OUT THE FORM, OR ANY ASPECT OF EXPORTING, IS PROVIDED BY THE EXPORT COUNSELING DIVISION IN WASHINGTON, D.C. AT (202) 482-4811 OR THE WESTERN REGIONAL OFFICE IN NEWPORT BEACH, CALIFORNIA AT (714) 660-0144.

LICENSE EXCEPTIONS

BE AWARE THAT THE LICENSING REQUIREMENTS FOR SOME DESTINATIONS MAY BE OVERCOME BY ANY LICENSE EXCEPTION FOR WHICH YOUR ITEMS QUALIFY. SEE PART 740 OF EAR FOR INFORMATION ON LICENSE EXCEPTIONS. THE LICENSE AVAILABLE COLUMN ON THIS FORM LISTS ONLY THOSE LICENSE EXCEPTIONS OF THE SET GBS, CIV, CTP, TSR WHICH ARE APPLICABLE TO YOUR ITEMS. OTHER LICENSE EXCEPTIONS MAY APPLY, DEPENDING UPON THE CIRCUMSTANCES OF YOUR INTENDED TRANSACTION.

EXPORT CONTROL CLASSIFICATION NUMBERING SYSTEM (ECCN)

THE ECCN NUMBERING SYSTEM IS FOUND IN THE COMMERCE CONTROL LIST (CCL) PART 774 OF THE EAR. THE CCL IS A COMPREHENSIVE LIST THAT IDENTIFIES ALL ITEMS CONTROLLED AND LICENSED BY COMMERCE. WITHIN THE CCL, ENTRIES ARE IDENTIFIED BY AN ECCN. EACH ENTRY SPECIFIES THE LICENSE REQUIREMENTS FOR THE ITEM AND THE REASON(S) FOR CONTROL. PLEASE CONSULT PARTS 738 AND 774 OF THE EAR FOR SPECIFIC INFORMATION ON ECCNS.

SHIPPERS EXPORT DECLARATION (SED)



**UNITED STATES DEPARTMENT OF COMMERCE  
BUREAU OF INDUSTRY AND SECURITY  
WASHINGTON, D.C. 20230**

WHEN AN EXPORT IS MADE, IT IS NECESSARY FOR THE EXPORTER TO SHOW ON THE SHIPPERS EXPORT DECLARATION (FORM 7525-V) IN BLOCK 27 EITHER THE LICENSE NUMBER, THE APPLICABLE LICENS EXCEPTION SYMBOL OR THE SYMBOL NLR. FORM 7525-V IS AVAILABLE FROM THE SUPERINTENDENT OF DOCUMENTS, U.S. GOVERNMENT PRINTING OFFICE OF WASHINGTON, D.C. 20402, AND FROM EXPORT ADMINISTRATION DISTRICT OFFICES (U.S. DEPT. OF COMMERCE).

CATHERINE PRATT  
DIVISION DIRECTOR

FOR INFORMATION CONCERNING  
THIS CLASSIFICATION CONTACT  
ANITA ZINZUVADIA  
PHONE #: 202-482-3772  
BIS/EA/STC/IT