Freescale Semiconductor
Product Brief

Document Number: C29xPB
Rev. 1, 07/2015

Freescale C29x Crypto Coprocessor Family Product Brief

1 Introduction

The Freescale C29x crypto coprocessor family consists of 3 high performance crypto co-processors 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 secure transactions possible. By providing public key acceleration, C29x enables network and data center infrastructure to handle the increasing rates of public key operations driven by IKE, SSL, DNSSEC, and secure BGP while simultaneously supporting the longer key lengths mandated for modern encryption.

Longer key lengths are a significant performance issue. The United States National Institute of Standards and Technology's (NIST) recommends replacing RSA 1024b keys with 2048b keys all together by 2013. Doubling the length of a RSA key increases the computational complexity by 5x or more. If a system needs thousands of transactions per second or more, using C29x for public key offload is the most cost effective means of meeting requirements.

Many modern multi-core SoCs, including those offered by Freescale, offer cryptographic acceleration, however the crypto hardware is oriented toward bulk encryption performance. The performance level of the integrated public key acceleration is generally sufficient for applications with modest session establishment requirements, but Web 2.0 systems such as application delivery controllers, network

Contents

admission control appliances and remote access gateways must deal with far more connections per second, and integrated public key acceleration becomes a performance bottleneck. C29x complements integrated bulk encryption acceleration, while allowing these different cryptographic functions to scale independently.

While primarily targeted toward public key operations, C29x does offer bulk encryption and hashing, including security header and trailer processing for IPsec and SSL.

This product brief provides an overview of the Freescale C29x family of crypto coprocessor features, and examples of C29x usage.

2 Application examples

The C29x family devices are designed for the following two primary use cases:

- Public key calculator
- Secure key management module

2.1 Public key calculator

The most obvious use of a cryptographic coprocessor optimized for public key operations is to off-load public key operations from a host CPU.

When operating in this mode, C29x connects to the host via PCIe, with C29x requiring no external memory; neither NVRAM nor DDR, and generally no peripheral ICs.

The host handles packet Rx and Tx functions, classification, protocol termination, and so on, and defines the operations it wants C29x to perform via descriptors.

In addition to public key operations, C29x can also support bulk encryption and hashing, including security header and trailer processing for IPsec and SSL.

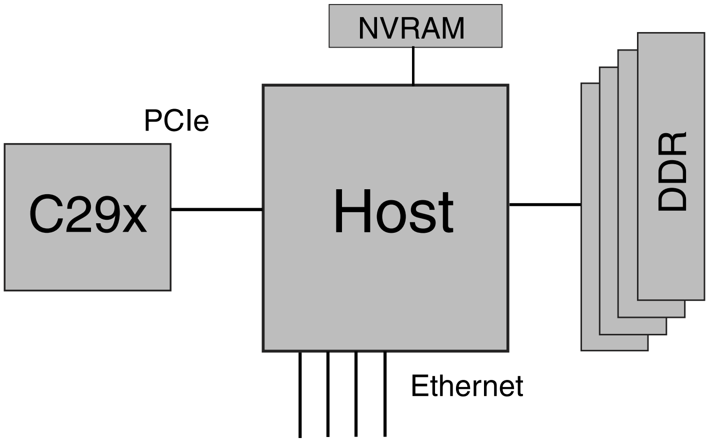

Figure 1. C29x operating as PK Calculator

2.2 Secure key management module

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.

Tamper detection and secure debug round out the Trust Architecture feature set. A more complete description of the Trust Architecture can be found in Freescale's white paper: *An Introduction to the QorIQ Platform's Trust Architecture*.

As shown in the following figure, when operating as a secure key management module, the C29x is a processing subsystem, complete with its own non-volatile memory, DDR, and optionally ethernet interfaces to either the external world or as a connection to the host. C29x can also be connected to the host via PCIe.

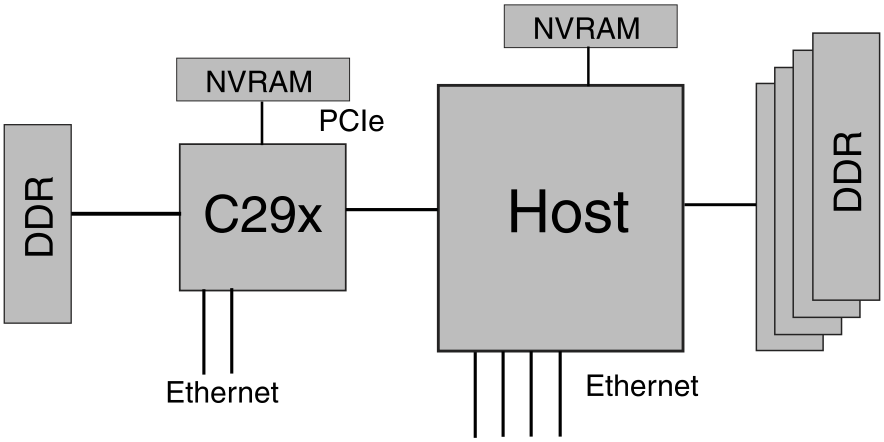

Figure 2. C29x operating as secure key management module

C29x is also capable of acting as a host. In such cases, C29x and its memories can either constitute a stand-alone system, or C29x can be the host/management processor for a high performance encrypting datapath, where NPUs or ASICs perform bulk encryption using keys negotiated (and securely managed) by C29x.

3 C29x family and features

C29x family consists of 3 family members; the C291, C292, and C293. All devices are pin compatible. A logical block diagram of the highest performing family member, C293, is shown below.

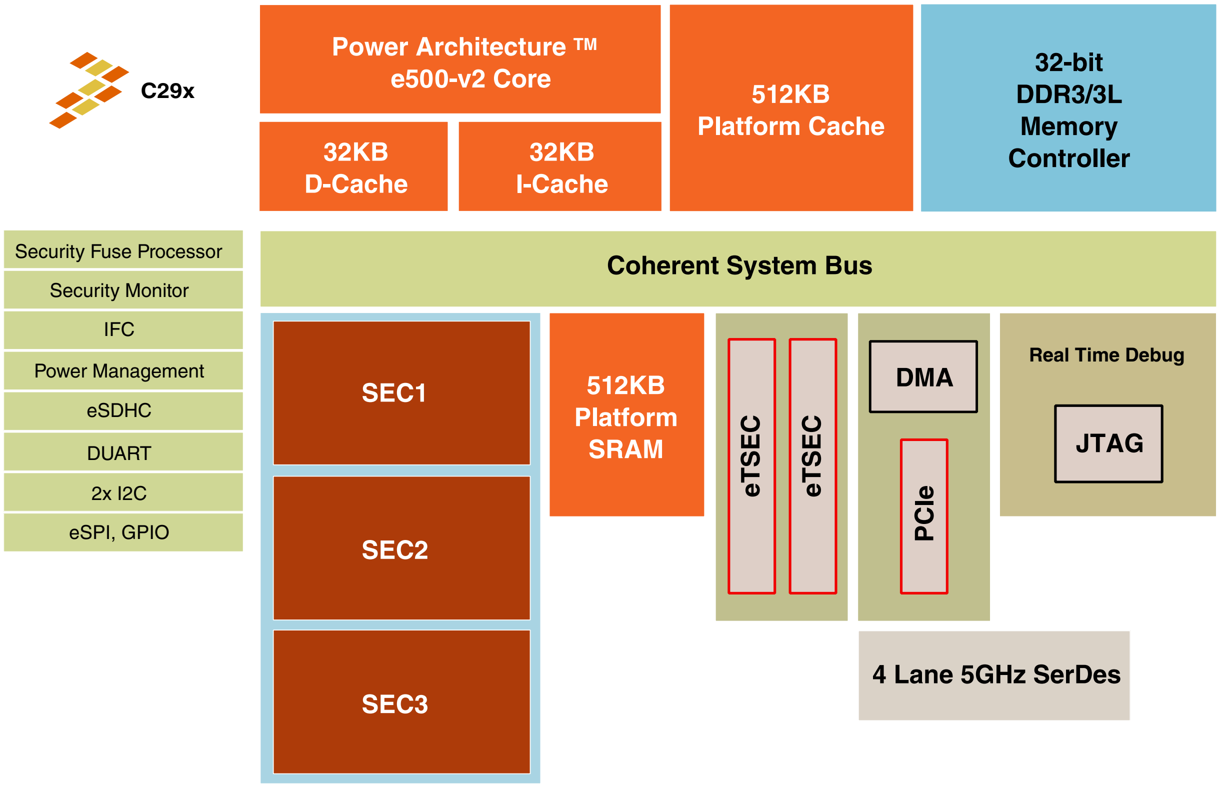

Figure 3. C29x logical block diagram

A summary of key performance metrics is shown in table below:

Table 1. C29x family key metrics

	C291	C292	C293
CPU	667 MHz	1 GHz	1.2 GHz
SEC	267 MHz	333 MHz	400 MHz
DDR	800 MHz	1067 MHz	1.2 GHz
2048b RSA Private Key	8,461	17,587	32,907
Bulk Encryption (AES-HMAC-SHA-1 for SSL or Ipsec)	6 Gbps	9 Gbps	12 Gbps

The above bulk encryption performance is system level throughput considering PCIe bandwidth and overhead. Full performance metrics for each device are provided in Performance.

Table 2. Typical power consumption

	C291	C292	C293
Security engines	1	2	3
Typical power (65C)	~6 W	~12 W	~18 W
2048 bit RSA KOPS/sec	8	18	32

3.1 Features

Common features of C29x products include:

- CPU and cache complex
  - 32b e500v2 Power Architecture® core
  - 32KB I and D caches
  - 512 KB L2 cache
  - Hardware cache coherency
- 512KB platform SRAM
- Up to three SEC (Security Engine) accelerator block(s)
  - See SEC details
- One PCIe Gen 2.0 controller
  - x1, x2, x4
- Main memory interface (optionally disabled in PK calculator use case)
  - 16/32-bit DDR3/3L controller with ECC
  - Supports up to 4GBytes main memory in single bank
  - Dual-stacked and quad-stacked DDR devices also supported
- Additional memory interfaces (optionally disabled in PK calculator use case)
  - Integrated flash controller
    - Supporting NOR and NAND (SLC and MLC) flash interfaces
    - Maximum of 8 banks, with a maximum of 256 MB of system memory mapped on each bank
  - Enhanced secure digital host controller (SD/MMC) which can be used for booting device using on chip ROM
- Network interfaces (disabled in PK Calculator use case)
  - Two enhanced three speed ethernet controller (eTSEC) supporting 10/100/1000Mbps
  - Supports RGMII/RMII interfaces
- Trust architecture, supporting;
  - Secure boot
  - Secure debug
  - Tamper detection
  - Provisioning with one time programmable fuses
  - Hardware secret key protection
  - Option for battery backed secret key
  - Memory and register Access Control
  - Only supported in secure key management module use case NVRAM
- Slow speed interfaces (optionally disabled in PK calculator use case)
  - Dual I2C controllers
  - SPI controller used for booting with internal ROM, supporting Atmel Rapid-S and Winbond dual read interface
  - Two UARTs
  - 64-bit GPIO
- Additional logic
  - Programmable Interrupt Controller
  - One four channel DMA
- Power Management supporting following modes
  - e500v2 modes
    - Sleep: core clock off, snooping off, cache flushed, clock to selected blocks switched off
    - Nap: core logic idle, no snoops
    - Doze: Core logic idle
  - Software transparent clock gating of SoC logic
  - Static disable of logic blocks, including SEC 1 and SEC 2
- Package
  - 783 pin FC-PBGA
  - 29x29mm, 1.0mm pitch

3.2 SEC details

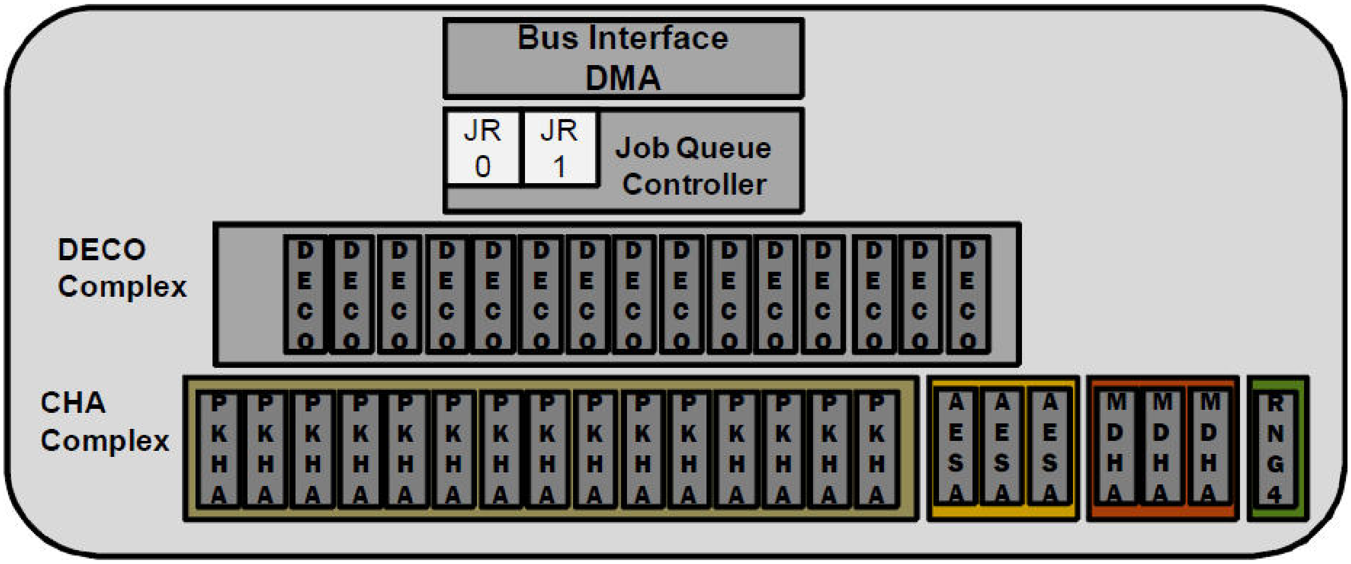

Figure 4. SEC logical block diagram

Each SEC block supports the following functionality:

- DMA for bus master operation
- Job Queue Controller with two Job Rings
- (15) Descriptor Controllers (DECOs)
  - Responsible for executing Descriptors and managing sequencing of keys, context, and data through the various CHAs
  - Performs header and trailer processing as defined by the descriptor
- Crypto Hardware Accelerators (CHAs)
- (15) Public Key Hardware Accelerators (PKHA) supporting the following key lengths and routines
  - Modular Arithmetic in support of RSA and Diffie-Hellman (to 4096b)
  - Elliptic curve cryptography (to 1024b)
    - Point math over a prime field (Fp)
    - Point math over a binary field (F2m)
  - Routines
    - Modular Addition (A + B) mod N
    - Modular Subtraction 1(A - B) mod N
    - Modular Subtraction 2(B - A) mod N
    - Modular Multiplication (A x B) mod N
    - Modular Exponentiation AE mod N
    - Modular Simultaneous Exponentiation A^E0 * B^E1 mod N
    - Modular Reduction A mod N
    - Modular Inversion A-1 mod N
    - ECC Point Add P1 + P2
    - ECC Point Double P1 + P1
    - ECC Point Multiply E x P1
    - Montgomery Radix Constant R2 mod N
    - Greatest Common Divisor GCD(A,N)
    - Primality Test Miller-Rabin

        - DSA Sign
        - DSA Verify
    - All routines with timing equalization to defeat side channel timing attacks
- (1) Random Number Generator
    - NIST certified DRBG and SHS implementation
    - DRBG Cert #94
    - SHS Cert #1455
        - SHA-256 with Prediction Resistance support.
- (3) Advanced Encryption Standard Accelerators (AESA)
    - Key lengths of 128-, 192-, and 256-bit
    - ECB, CBC, CTR, CCM, GCM, CMAC, OFB, CFB, and XTS
    - Differential Power Analysis Resistant design
- (3) Message Digest Hardware Accelerators (MDHA)
    - SHA-1, SHA-2 256,384,512-bit digests
    - MD5 128-bit digest
    - HMAC with all algorithms

3.3 Trust architecture overview

The Trust architecture consists of a set of hardware and software techniques designed to support a trusted boot environment and to maintain the trusted environment during runtime.

When operating in the Secure key management module use case with attached non-volatile memory, C29x supports a secure boot option, in which, the system developer digitally signs the code to be executed by C29x, and C29x validates that code to insure that only an unaltered version of that code runs on the Secure Key Management Module. C29x also supports protected internal and external storage of developer-provisioned sensitive instructions and data. For example, a system developer may provision each C29x with a number of RSA private keys to be used in mutual authentication and key exchange. These values would initially be stored as encrypted blobs in external non-volatile memory, but following secure boot, these values can be decrypted into on-chip protected memory.

Session keys, which may number in the thousands to tens of thousands, are not good candidates for on-chip storage, so C29x offers session key encryption. Session keys are stored in main memory, and are decrypted (transparently to software and without impacting SEC throughput) as they are brought into the SEC for decryption of session traffic.

4 Performance

The following sections and tables provide detailed C29x family device performance. All numbers are expressed as operations per second with the exception of bulk encryption which is measured in Gbps. The bulk encryption throughput represents SEC capability, actual system throughput will be determined by both SEC performance and I/O bandwidth.

Note that many performance numbers were obtained in simulation, and include all SEC operations beginning with reading a descriptor pointer from an input job ring and ending with the SEC’s job completion status write to the output job ring. Software overheads for security protocol processing and descriptor creation are not included. The 2048b RSA private key operations/sec result for all three family members has been measured on initial silicon, and is highlighted in each table. The measured result exceeded the simulated result by ~4%.

4.1 C291

Table 3. C291 detailed performance

1024b RSA Public	366,000[1]	1024b RSA Private	30,830
2048b RSA Public	152,509	2048b RSA Private	8,461
4096b RSA Public	44,953	4096b RSA Private	1,800
Diffie Helman Group 14 (Exp 220b)	13,656	Diffie Helman Group 14 (Exp 320b)	9,992
Diffie Helman Group 16 (Exp 300b)	2,930	Diffie Helman Group 16 (Exp 480b)	1,931
ECP Group 256 Verify	11,111	ECP Group 256 Sign	15,201
ECP Group 384 Verify	5,628	ECP Group 384 Sign	7,728
ECP Group 521 Verify	2,757	ECP Group 521 Sign	3,762
B-283 Verify	12,451	B-283 Sign	21,057
B-409 Verify	6,732	B-409 Sign	11,564
B-571 Verify	3,981	B-571 Sign	6,961
PRF (Pseudo random function)	281,250		
Bulk Encryption	AESHMAC-SHA-1		6 Gbps

NOTE

1. Approximate jobs/sec limit for the C29x host driver and C29x firmware

4.2 C292

Table 4. C292 Detailed Performance

1024b RSA Public	458,000[1]	1024b RSA Private	64,086
2048b RSA Public	317,013	2048b RSA Private	17,587
4096b RSA Public	93,442	4096b RSA Private	3,742
Diffie Helman Group 14 (Exp 220b)	30,687	Diffie Helman Group 14 (Exp 320b)	22,454
Diffie Helman Group 16 (Exp 300b)	6,584	Diffie Helman Group 16 (Exp 480b)	4,340
ECP Group 256 Verify	27,714	ECP Group 256 Sign	37,918
ECP Group 384 Verify	14,038	ECP Group 384 Sign	19,276
ECP Group 521 Verify	6,877	ECP Group 521 Sign	9,384
B-283 Verify	31,058	B-283 Sign	52,524
B-409 Verify	16,792	B-409 Sign	28,844
B-571 Verify	9,929	B-571 Sign	17,363
PRF (Pseudo random function)	~458,000[1]		
Bulk Encryption	AESHMAC-SHA-1		12 Gbps

NOTE

1. Approximate jobs/sec limit for the C29x host driver and C29x firmware

4.3 C293

C293 performance for 1024, 2048, and 4096b RSA private key operations have been measured on first silicon.

Table 5. C293 Detailed Performance

1024b RSA Public	~550,000[1]	1024b RSA Private	117,499
2048b RSA Public	~550,000[1]	2048b RSA Private	32,907
4096b RSA Public	168,365	4096b RSA Private	6,964
Diffie Helman Group 14 (Exp 220b)	55,292	Diffie Helman Group 14 (Exp 320b)	40,458
Diffie Helman Group 16 (Exp 300b)	11,862	Diffie Helman Group 16 (Exp 480b)	7,819
ECP Group 256 Verify	49,935	ECP Group 256 Sign	68,321
ECP Group 384 Verify	25,293	ECP Group 384 Sign	34,731
ECP Group 521 Verify	12,932	ECP Group 521 Sign	16,908
B-283 Verify	55,961	B-283 Sign	94,638
B-409 Verify	30,255	B-409 Sign	51,972
B-571 Verify	17,981	B-571 Sign	31,286
PRF (Pseudo random function)	~550,000[1]		
Bulk Encryption	AESHMAC-SHA-1		16 Gbps

NOTE

1. Approximate jobs/sec limit for the C29x host driver and C29x firmware
2. RSA performance with CRT (Chinese Remainder Theorem)
3. DH performance includes two modular exponentiations

5 Software and development tools

C29x software consists of host and device components. Reference host software will be provided for Linux, and consist of a C29x Crypto/PK driver and crypto enablement components. The device software, which executes on C29x e500 CPU, consists of a lightweight RTOS and firmware. C29x interacts with a host processor over a PCIe interface and generally functions as an endpoint. The main software components on C29x include firmware that facilitates initialization and boot, the dispatcher that processes job requests from the host against a SEC engine farm, and a device management agent that handles management related functionality.

5.1 PK calculator software model

Figure below shows the software model for C29x's PK calculator use case. Applications running on the host processor make use of the C29x through the OpenSSL library. C29x's device driver is ported (by Freescale) to the OpenSSL Engine interface, so that requests for crypto services result in creation of a SEC descriptor and placement of that descriptor on a C29x software ring. The host driver uses PCIe Message signalled interrupts (MSIs) to advise C29x e500 core that new descriptors have been added to the software ring.

In C29x products with >1 SEC (C292 and C293), dispatcher firmware running on the e500 core selects the best SEC to process the descriptor and adds a descriptor pointer to that SEC's input job ring. When the SEC updates the output job ring, the e500's dispatcher firmware checks completion status, and notifies the host driver (via MSI) that the request has been processed. C29x host based driver and device based firmware are designed to move data in a push-push model, eliminating high latency PCIe reads.

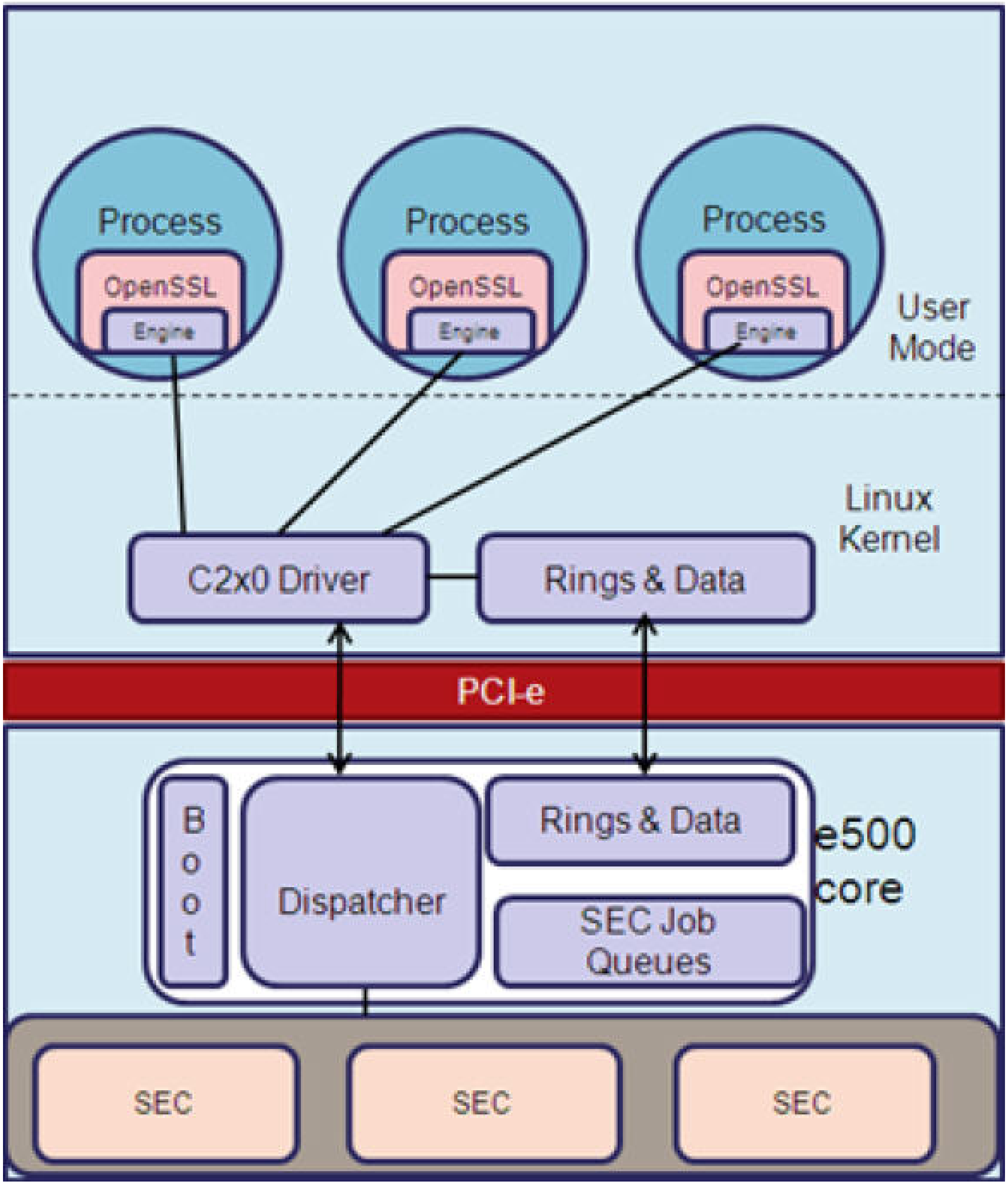

Figure 5. C29x PK Calculator software model

5.2 Secure key management module software model

In the secure key management use case, the C29x's lightweight RTOS is replaced by Linux, and C29x can be used like any QorIQ communications processor operating as a PCIe end-point.

NOTE

C29x can also operate as a complete stand-alone appliance without a PCIe connection to a host. Developers can wrap their own key management software around the dispatcher and SEC job ring management firmware.

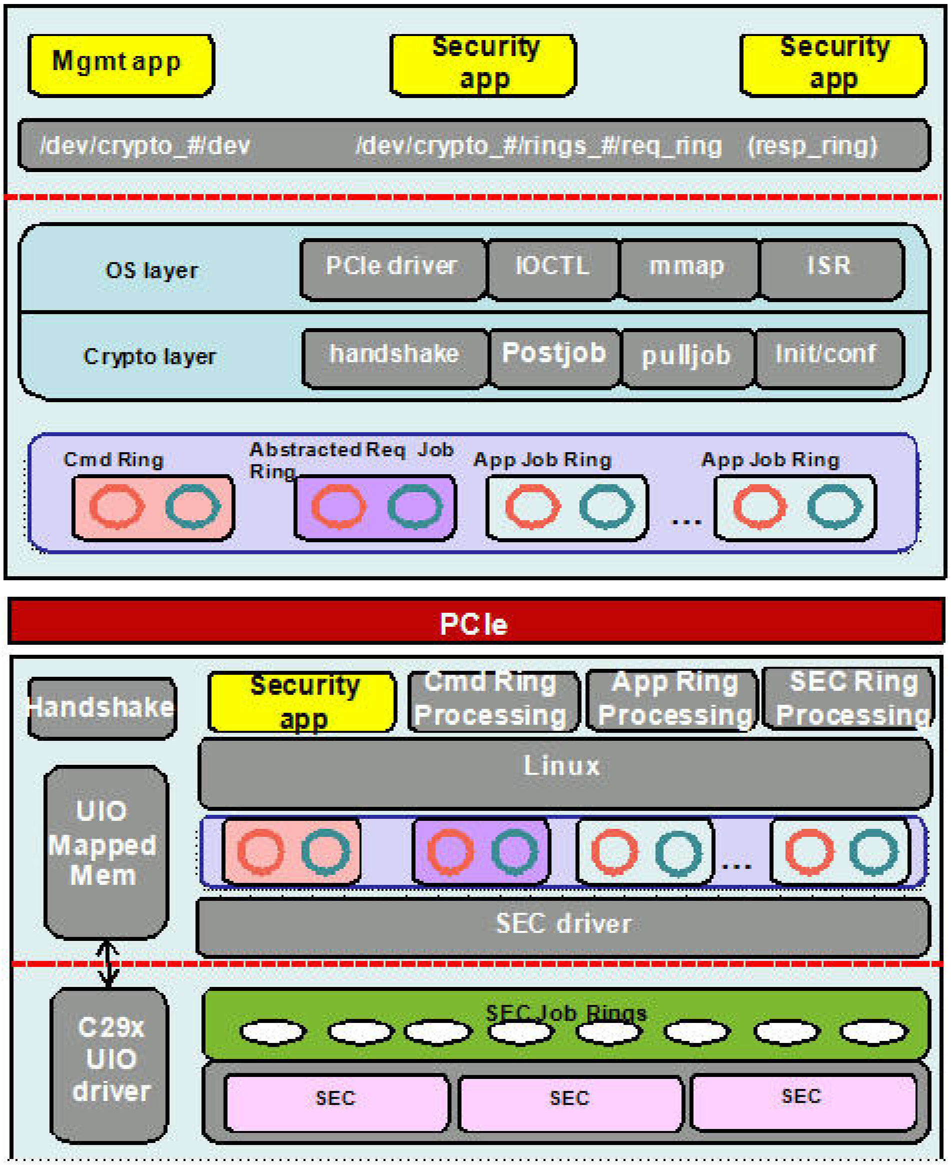

Figure 6. C29x SKMM software model

5.3 C29x development system

As shown in the figure below, Freescale’s development system for C29x is based on a half height PCIe card form factor. This card can be plugged into standard PCIe card slots or operate as a small stand-alone appliance (12V DC power supply). The development system features all external devices required for the secure key management module use case (DDR, Flash, ethernet PHYs), however these can be disabled for PK calculator operations.

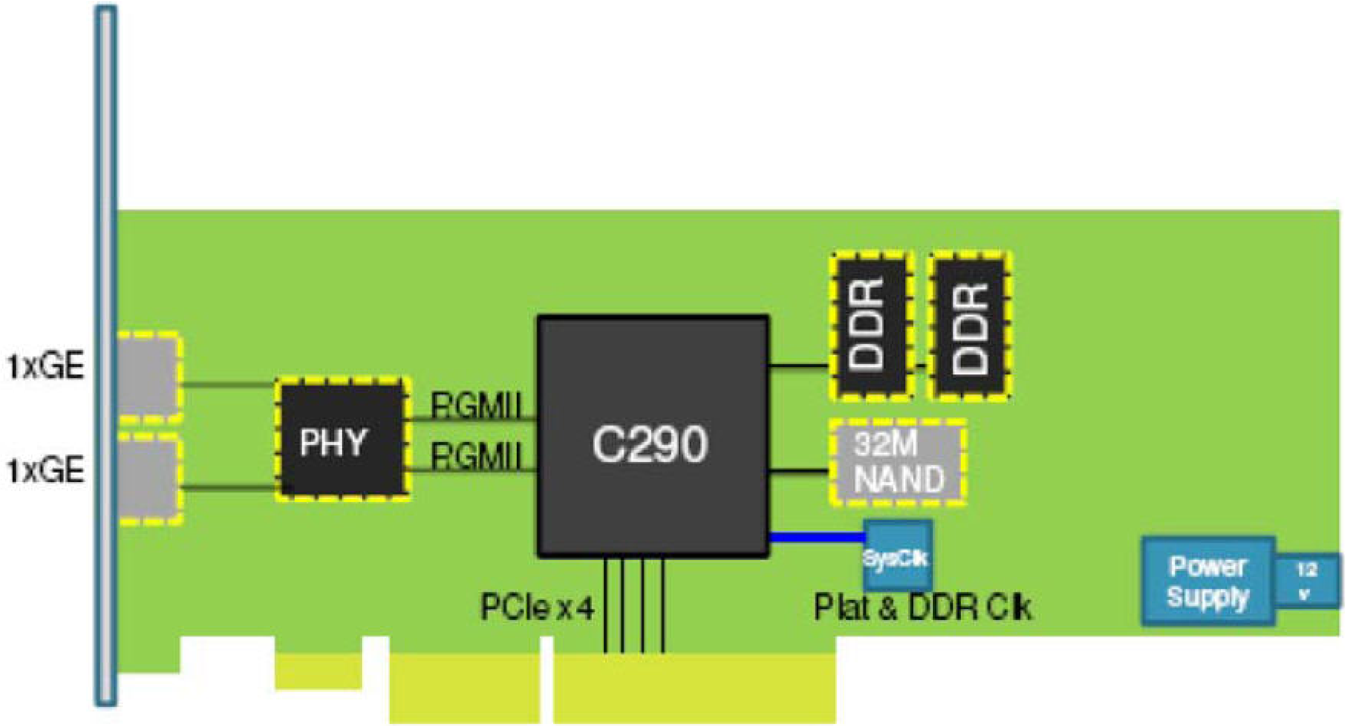

Figure 7. C29x half height PCIe card development system

5.4 Ecosystem

Freescale is committed to an open ecosystem of hardware and software providers for C29x. Please contact Freescale for more information about partners offering cost optimized PK Calculator PCIe cards, FIPS certified secure key management modules leveraging the Trust Architecture, and value added software solutions relevant to both use cases.

6 NDA Data Sheet and Samples

Additional technical specifications not included in the Product Brief can be accessed under NDA by contacting your local Freescale or Freescale Distribution field personnel.

7 Revision history

This table summarizes revisions to this document

Table 6. Document revision history

Revision	Date	Description
1	07/2015	Updated the following tables: Table 1, Table 3, Table 4 and Table 5
0	10/2013	Initial public release

How to Reach Us:

Home Page:
freescale.com

Web Support:
freescale.com/support

Information in this document is provided solely to enable system and software implementers to use Freescale products. There are no express or implied copyright licenses granted hereunder to design or fabricate any integrated circuits based on the information in this document. Freescale reserves the right to make changes without further notice to any products herein.

Freescale makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does Freescale assume any liability arising out of the application or use of any product or circuit, and specifically disclaims any and all liability, including without limitation consequential or incidental damages. “Typical” parameters that may be provided in Freescale data sheets and/or specifications can and do vary in different applications, and actual performance may vary over time. All operating parameters, including “typicals,” must be validated for each customer application by customer's technical experts. Freescale does not convey any license under its patent rights nor the rights of others. Freescale sells products pursuant to standard terms and conditions of sale, which can be found at the following address: freescale.com/SalesTermsandConditions.