C29x Crypto Coprocessors: Software and Implementation

FTF-NET-F0065

Jim Bridgwater | Product Manager
Sam Siu | Application Engineer

APR. 2014
Agenda

• C290 Crypto Coprocessor Overview
  – Features (public key acceleration)
  – Trust Architecture (key protection)
  – Use cases

• Software Development Kit (SDK)
  – Programming model
  – Drivers (firmware and PCIe driver)
  – Enablement applications

• Performance Analysis (Offload and CPU Utilization)
Secure Network Traffic is Growing … Fast!

Cybercrime is a **double digit** growth industry & government surveillance is a concern

Online retail growth at **15%** CAGR through 2016

**40%** of households to use online banking by 2014

Google:
- All searches use **SSL**
- All emails encrypted
- Upgraded to **2k keys**

Facebook supports **HTTPS** and **forward secrecy**

BYOD: Enterprise Tablet adoption growing at **50%** a year

Global cloud traffic is growing **12x** in 5 years
Security is Everywhere and Must Scale

**Data Center:**
Large amounts of SSL traffic terminated in the **Application Delivery Controller** to help keep the datacenter efficient.

**Enterprise:**
**Security Appliances** ensure secure access through network admission control, firewall and deep packet inspection in corporations, government and schools.

**Other**
- Critical security infrastructure such as Hardware Security Modules used in finance and banking
- Mobility management including the authorization, authentication and accounting (AAA) server
Scaling is Challenged Without Acceleration

• Network Admission Control, IPsec, and SSL are becoming ubiquitous
  – All use asymmetric cryptography (aka Public Key or PK) for authentication and key exchange
  – Public key “big number” math is extremely CPU-intensive

• **Requirements only increasing:**
  – RSA1024-bit keys were phased out in 2013
  – RSA 2048-bit keys require 4X computing power
Internet Security Basics – How TLS (Formerly SSL) Works

1. **Authentication**
   - Server & Client exchange security certificates as proof of identity, including each other’s public key
   - Involves “Signing” with private key & “Verifying” with public key
   - Public-private key pair are asymmetric: private key is much larger than public key
   - Uses RSA algorithm, moving from 1024b to 2048b key length (Elliptic Curve Cryptography also used, less common)

2. **“Master Secret” creation**
   - Client creates pre-master secret, encrypts it with server’s public key, sends it to server
   - Server decrypts pre-master secret with its private key, uses it to generate master secret.

3. **Session Key creation**
   - Client and Server use the master secret to generate the symmetric session keys
   - Symmetric session keys used for bulk encryption / IPSec (normally 256-bit AES)

**Diagram Notes**
- AES-HMAC-SHA2 commonly used for encrypting the HTTP payloads (aka TLS records)
- Signing and decrypting are the most difficult operations in connection set-up, limit HTTPS connection rate
C29x Family Overview

- PCIe based public key accelerator with scalable performance and power
- Optimized for public key offload
  - Leading performance/dollar
  - Lower power
- Trust architecture to enable secure key management

<table>
<thead>
<tr>
<th>Security Engines</th>
<th>C291</th>
<th>C292</th>
<th>C293</th>
</tr>
</thead>
<tbody>
<tr>
<td>Typical Power (65C)</td>
<td>~6W</td>
<td>~12W</td>
<td>~18W</td>
</tr>
<tr>
<td>2048 bit RSA KOPS/sec</td>
<td>8</td>
<td>18</td>
<td>32</td>
</tr>
</tbody>
</table>
PE2SFC293—Silicom Security Accelerator

Key Features:
• Single C293 crypto coprocessor
• PCI Express® Gen-2 x4 connector supporting x4, x2 and x1 links
• Dimensions: PCIe low profile, 68.9mm x 167.65mm
• Power consumption: ~22W
• Environment: 0 °C to 50 °C
• No external power needed
• High-performance public key processor
Trust Architecture
C29x Crypto Coprocessor Family - Trust Architecture 2.0

Features:
- Secure boot
- Secure debug
- External tamper detect (system defined)

- Zeroizable, one-time programmable master key
- Multiple session key support

- Power Architecture e500-v2 Core
- 512 KB Platform Cache
- 32-bit DDR3/3L Memory Controller

- 32 KB D-Cache
- 32 KB I-Cache

- Coherent System Bus
- CCSR Access Controller

- Battery Back-up
- Internal Boot ROM
- Security Fuse Processor
- Security Monitor
- IFC
- Power Management
- SD/MMC+
- 2x DUART
- 2x I2C
- SPI, GPIO

- External Tamper Detect

- SEC 1 (C291,2,3)
- SEC 2 (C292,3)
- SEC 3 (C293)

- 512 KB Platform SRAM
- DMA
- PCIe
- eTSEC
- eTSEC
- Real Time Debug
- JTAG
- 4 Lane 5 GHz SerDes
Code Integrity via the Trusted Boot Process

OEM System Provisioning

- System Image
- Signature
- Public Key
- D, N
- Private Key Encryption
- Message Digest Hash
- E, N
- Public Key

Note: Program and Signature may also be encrypted for IP protection
Private Key has to be carefully managed and protected

Trusted Boot

- System Image
- Signature
- Public Key
- D, N
- Private Key Encryption
- Message Digest Hash
- E, N
- Public Key
- Verify Key
- Public Key Decryption
- Compare Hash Sum
- Authentication Result
- Hash^E mod N

Internal Secure Boot Code
Secure Boot Hardware State Diagram

- **Secure Boot?**
  - **Non Secure**
    - **Soft Fail**
      - Security Violation
      - If Hard Fail Enable
      - System Reset
  - **Secure Fail**
    - Hard Fail
    - Security Violation
    - Hard Fail
    - Hard Fail

- **Trusted State**
  - **Authorized Image**
  - **Secure State**
    - No Security Violation
    - Access secure vault (BLOB)
    - OTPMK KEK

- **Any Image**
  - **Secure Boot**
  - **Hard Fail**
    - No Key Usage (OTPMK & KEK)
    - Vault is CLOSE

- **System Reset**
Use Cases
C290 Family Solutions – Public Key Offload

- Embedded processor or plug-in PCIe options for rapid time to market
- A broad range of performance from 8-30K/tsp for 2048-bit RSA
- Third-party support for x4 device PCIe cards performing >120K/tsp
- Host connection via a PCIe gen2 x4 lane interface
- No external memory (NVRAM or DDR) needed
- Freescale provides Linux® host and drivers with SDK
- OpenSSL supported via the simple API

Public Key Calculator
- PCIe look-aside co-processor
- Boot over PCIe (no secure boot)
- Host driver + FSL Firmware on C2x0
C290 Family Solutions - Hardware Security Modules

The HSM generates, manages and stores keys in a single secure unit.

C290 coprocessor uses the **Trust Architecture** for:

- Secure boot insuring that factory loaded software can be used
- Secure storage insuring that only factory loaded keys can be used
- Tamper detection and secure debug for physical security

C290 coprocessor enables a processing subsystem with:

- Dedicated non-volatile memory
- Dedicated DDR
- High-performance PCIe gen2 x4 lane connection to the host
- Optional Ethernet interfaces for user or host connection

Secure Key Management Module

- PCIe look-aside co-processor
- Optional Ethernet interface
- Secure boot from local NVRAM
- Host driver + FSL Firmware + OEM/3rd party applications on C2x0
C29x Crypto Coprocessor - Performance Comparison

- Public key and private key computation (CPS)

![Graph 1: 1024b Pub Key, 2048b Pub Key, 4096b Pub Key]

- C291
- C292
- C293

![Graph 2: 1024b Pri Key, 2046b Pri Key, 4096b Pri Key]

- C291
- C292
- C293
C293 Crypto Coprocessor Performance Benefits

# openssl speed rsa --engine cryptodev --elapsed --multi 200

CPU Utilization

Ops/sec

- No offload Ops/Sec
- Offload Ops/Sec
- No offload % CPU
- Offload % CPU
C29x Crypto Coprocessor Programming Model
High-level Software Component View PK Calc

Multiple Rings
- Supports multiple applications or partitions on host
- Interrupt per ring

Ring properties
- Priorities
  - Strict priority
  - Round robin on same priority rings
- Affinity to hardware engines
- Order-preservation

Command Ring
- Configuration
- Statistics
- Diagnostics
SKMM has full SDK, not just host driver and firmware.

Requests for crypto services can come from Host or network interface.

When requests come from Host, process should be as similar to PK Calc as possible. One difference is SEC descriptor building will generally occur on the C29x coprocessor in SKMM.

Customers using C29x coprocessor as SKMM will only use our code for reference. Most will have high security OSes and their own hardened key management applications.
SKMM Software – Detailed View

- Basically leverage PK Calculator's design expect the followings:
  - C29x device secure boot itself from NOR flash
  - C29x driver runs in user space
  - C29x UIO driver maps L2 SRAM and outbound window space to user space
  - C29x driver initializes its own resources
  - C29x driver initializes SEC engine
  - Host driver post abstracted requests to C29x device
  - C29x driver uses poll mode to get the requests and use MSI interrupt to notify host of posting the results
  - C29x driver parse the abstracted requests, build the SEC job descriptors and add the descriptors to SEC engine
  - C29x driver use blob mechanism to protect the private key
Drivers
(Firmware and PCIe Driver)
High-level Software Component View

- **Functionality**
  - Public Key Acceleration
  - Bulk crypto w/ SSL Record Layer Offload

- **Software components on Linux® host**
  - Enhanced OpenSSL library
    - Synchronous & Asynchronous operations
    - SSL record layer offload
    - OpenSSL engine
  - FSL Crypto Acceleration Framework
    - Based on open source cryptodev
  - C29x driver and tools
    - fsl_crypto_offload_drv.ko
    - PCI CLI Tools

- **C29x Coprocessor Firmware**
  - Job dispatcher with multiple job rings
  - Boot over PCIe from host
Host Software Preparation

Step 1:
- Download Linux® kernel source
- Apply patch
- Build Linux image
- Reboot with new image

Step 2:
- Build Linux cryptodev
- Build c29x host driver
- Build c29x firmware with e500mc cross compiler (provided by Freescale Linux SDK)

Step 3:
- Build SSL library with new Linux cryptodev

Freescale C29x software bundle:
- Linux Kernel
- Linux Cryptodev
- C290 Driver - source
- C290 Firmware – source *

Open source
Freescale C29x crypto coprocessor software bundle

OpenSSL
SSL library
Enablement Applications
• Download the latest SDK (e.g. C293_PKC_SDK1.4_20130823.tar.bz2)
  - C29X-PCIe-Adapter-Quick-Start-Guide.pdf
  - C29x_Crypto_Offload_User_Guide.pdf
  - C29x_CLI_User_Guide.pdf
C29x Crypto Coprocessor - Firmware Build Configuration

- Verify config.mk
  - SDK_PATH =<installation path>
  - C293_EP = y
  - DEBUG_PRINT, INFO_PRINT, ERROR_PRINT = n
  - #Specifies whether host DMA support to be enabled /disabled in the driver
  - USE_HOST_DMA=n
  - vs
  - USE_SEC_DIRECT_READ=y

- Verify crypto.cfg
  
  <device>
  firmware:/etc/crypto/u-boot-sd.bin
  rings:3
  <ring>
  depth:16 /* Ring size */
  affinity:0 /* Sec engine affinity */
  priority:1 /* Relative priority of rings */
  order:0 /* Whether the ring processing is ordered or not */
  <end>
  ...
  ...
Driver Run Time Configurations

• The driver uses the following default settings:
  - Firmware binary at /etc/crypto/u-boot-sd.bin
  - Configuration file at /etc/crypto/crypto.cfg

• Driver options:
  - E.g.
    - `insmod fsl_crypto_offload_drv.ko dev_config_file=/etc/crypto/crypto.cfg`
    - `napi_poll_count=10 wt_cpu_mask=0x3 dma_channel_count=8`
    - `dma_channel_cpu_mask=0xff`

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Mandatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>dev_config_file</td>
<td>Device configuration file. Specifies all the configurations for the device, please see above section for details.</td>
<td>Y</td>
</tr>
<tr>
<td>napi_poll_count</td>
<td>Specifies the higher limit of the count for which worker threads should be polling.</td>
<td>N</td>
</tr>
<tr>
<td>wt_cpu_mask</td>
<td>Bit mask of CPUs on which worker threads needs to be scheduled.</td>
<td>N</td>
</tr>
<tr>
<td>dma_channel_count</td>
<td>DMA channel count for driver to use .</td>
<td>N</td>
</tr>
<tr>
<td>dma_channel_cpu_mask</td>
<td>Defines the distribution of channels to CPUs</td>
<td>N</td>
</tr>
</tbody>
</table>
OpenSSL Integration (x86 Host)

• Driver provides the crypto-offload to userspace applications through KCAPI (Kernel Crypto API)

• Cryptodev framework (CDF)
  - This is “/dev/crypto” interface for the application
  - This module needs to be compiled and inserted in the host
  - Standard CDF does not have PKC extensions; a version of CDF is extended for PKC and is maintained in the build

• Procedure to compile and insert CryptoDev Framework
  > cd <dir>/crypto_patches/x86_deps/cryptodev-linux-1.5_v-2
  > make
  > insmod /lib/modules/3.8.13-rt9-QorIQ-SDK-V1.4/extra/cryptodev.ko

• Procedure to compile openssl
  > cd <dir>/crypto_patches/x86_deps/openssl-1.0.1c_v-2
  > ./config -DHAVE_CRYPTODEV
  > make
  > make install
Summary
Trust and Secure

- C290 provides a trusted environment for public key accelerator with scalable performance and power.
- Optimized for public key offload
- Leader of performance/dollar

Key Management

Trust Architecture to protect the node

VPN Tunnel

SEC to accelerate protection of the channel
Introducing The QorIQ LS2 Family

Breakthrough, software-defined approach to advance the world’s new virtualized networks

New, high-performance architecture built with ease-of-use in mind
Groundbreaking, flexible architecture that abstracts hardware complexity and enables customers to focus their resources on innovation at the application level

Optimized for software-defined networking applications
Balanced integration of CPU performance with network I/O and C-programmable datapath acceleration that is right-sized (power/performance/cost) to deliver advanced SoC technology for the SDN era

Extending the industry’s broadest portfolio of 64-bit multicore SoCs
Built on the ARM® Cortex®-A57 architecture with integrated L2 switch enabling interconnect and peripherals to provide a complete system-on-chip solution
QorIQ LS2 Family

Key Features

High performance cores with leading interconnect and memory bandwidth
- 8x ARM Cortex-A57 cores, 2.0GHz, 4MB L2 cache, w/ Neon SIMD
- 1MB L3 platform cache w/ECC
- 2x 64b DDR4 up to 2.4GT/s

A high performance datapath designed with software developers in mind
- New datapath hardware and abstracted acceleration that is called via standard Linux objects
- 40 Gbps Packet processing performance with 20Gbps acceleration (crypto, Pattern Match/RegEx, Data Compression)
- Management complex provides all init/setup/teardown tasks

Leading network I/O integration
- 8x1/10GbE + 8x1G, MACSec on up to 4x 1/10GbE
- Integrated L2 switching capability for cost savings
- 4 PCIe Gen3 controllers, 1 with SR-IOV support
- 2 x SATA 3.0, 2 x USB 3.0 with PHY

Unprecedented performance and ease of use for smarter, more capable networks

SDN/NFV Switching

Data Center

Wireless Access
See the LS2 Family First in the Tech Lab!

4 new demos built on QorIQ LS2 processors:

- Performance Analysis Made Easy
- Leave the Packet Processing To Us
- Combining Ease of Use with Performance
- Tools for Every Step of Your Design