Open Virtualization Overview

Simply Secure

open virtualization

Open Virtualization

- First open source, free implementation for ARM® TrustZone®
- Comprehensive solution from secure boot to application management
- Supports all ARM architectures:
  - ARM11, Cortex-A8, A9 & A15

ARM®

Cortex™

Low-Power Leadership from ARM

open virtualization

Portable, Small Footprint

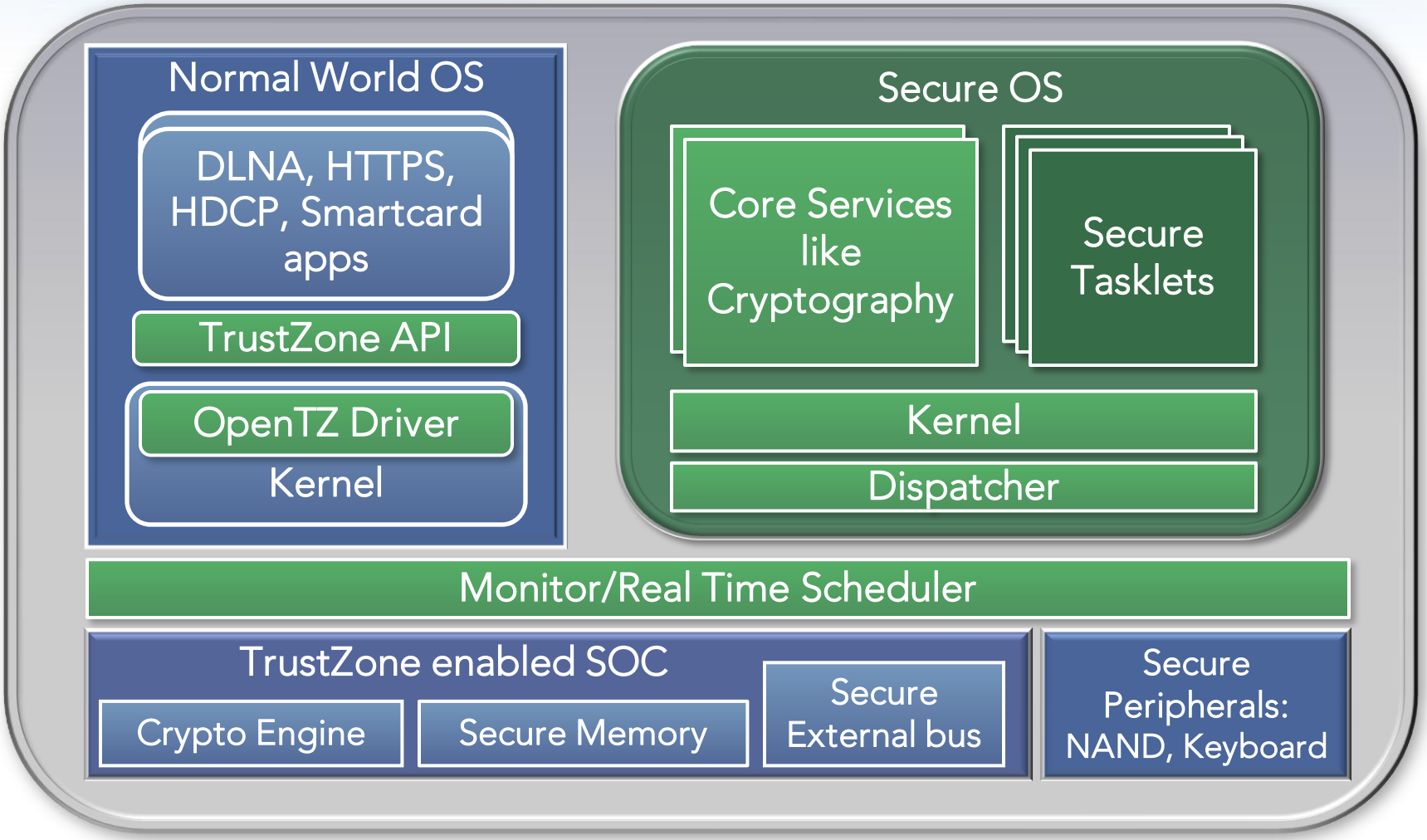
- Mixed mode architecture
  - Supports C, C++ and Java
  - Easy to integrate with Android and other mobile platforms

- Can be customized to fit on resource-constrained platforms

Supports Leading Platforms

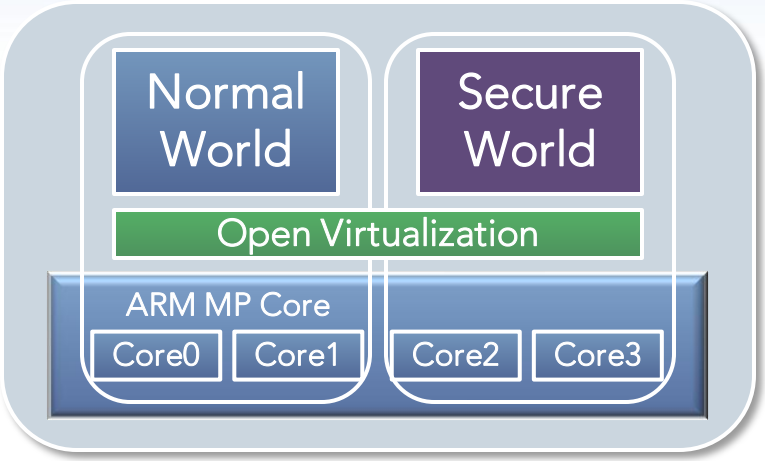
- Easy to develop and integrate with platforms like Linux, Android & BSD
- Written in C with GNU tools

Open Virtualization Architecture



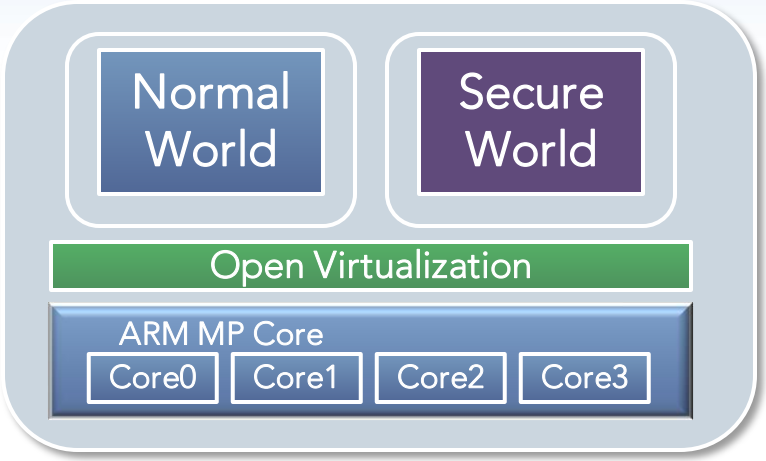
open virtualization

Multi-core Ready Options



Dedicated Cores for Secure and Normal World

- Satisfies size and performance constrained designs
- Ideally suited for high performance applications like media playback, transcoding



Secure and Non-secure Kernels Share Cores

- Provides maximum peak CPU bandwidth
- Both secure and non-secure kernels can utilize all available cores

open virtualization

Powerful, Purpose-built OS

- Flexible with Neon and VFP
  - Fully shared mode
  - Supports both “Secure” or “Normal” world
- Thwarts side channel attacks by protecting branch target buffers, TLBs, etc
- Supports several interrupt models
  - FIQ & IRQ in dedicated secure cores
  - FIQ only mode when sharing cores
  - Interrupt routing from secure to non-secure world

Simple, Small, Easy-to-Use

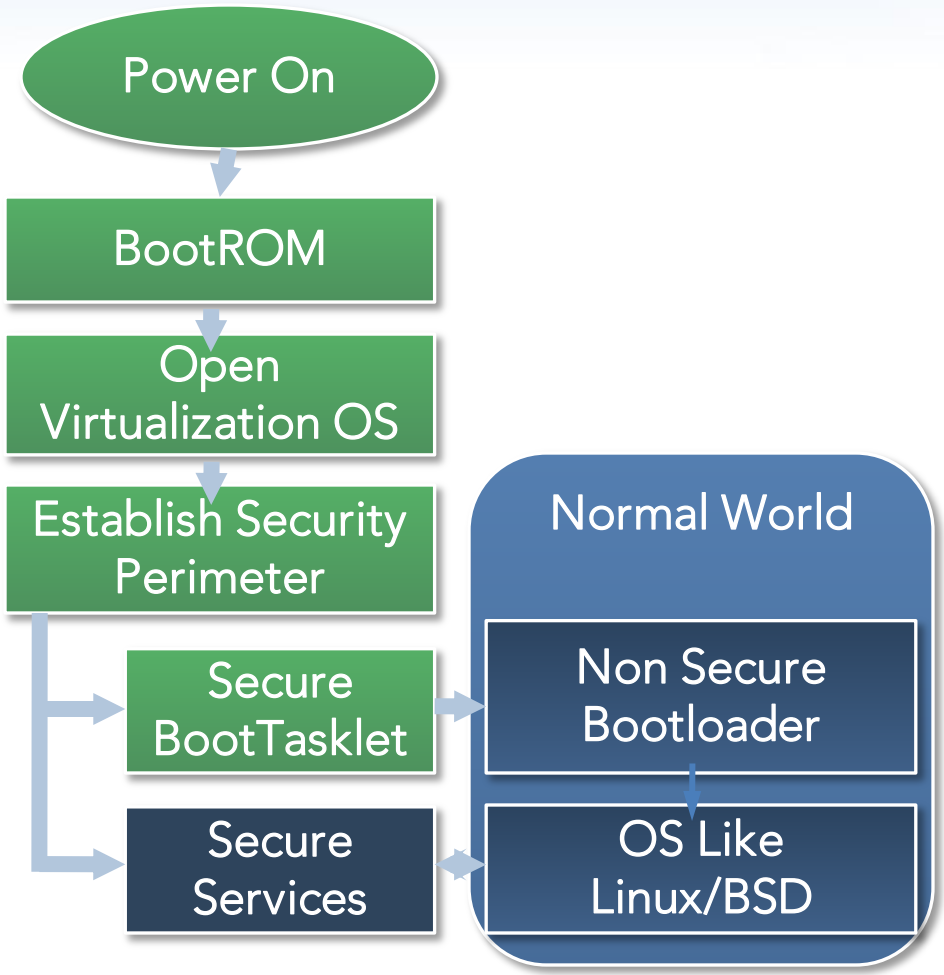
- Image can fit in small on-chip ROM
- Flexible scheduler: preemptive, cooperative
- Supports asynchronous IPC
- Stack overflow detection and profiling support
- High performance architecture with zero copy device drivers, fast context switching and cache lock down

Flexible Resource Control

- Supports:
  - Queues
  - Binary semaphores
  - Counting semaphores
  - Recursive semaphores
  - Mutexes with priority inheritance
  - Efficient software timers

Security Starts from Boot

- Secure perimeter starts with the bootloader
- Users can continue to use their preferred bootloader
- Security established before activating the bootloader
  - Keys, media and other assets are fully protected



Extensible Architecture

- Ready-to-use modules
- Open Virtualization API is available for both Bootloader and Linux
- Secure tasklets can perform key operations like decrypting OS images and upgrading firmware
- Multiple modes of operation support both TrustZone enabled and normal processors

Digital Rights Management

- Open Virtualization enables DRM, secure payment, and secure WiFi
  - Crypto and integrated with Linux OCF
  - Secure keypad and display
  - Protected key and content storage, authenticated flash

TrustZone
Security Foundation by ARM

open virtualization

Applications

1. Headless Gateway
   - Secure transcoding prevents valuable content from being snooped

2. Residential Gateway
   - Secure BSSID and other network provisioning
   - Defend against hackers and intrusions

open virtualization

Applications

1. Mobile Phones
   - Secure Payments
   - DRM Content protection
   - Isolate secure OS from normal world OS
2. IP Set-top-box, Media Players
   - DRM, Content Protection

Thank you!

developers@openvirtualization.org

open virtualization