Android Virtualization from Sierraware

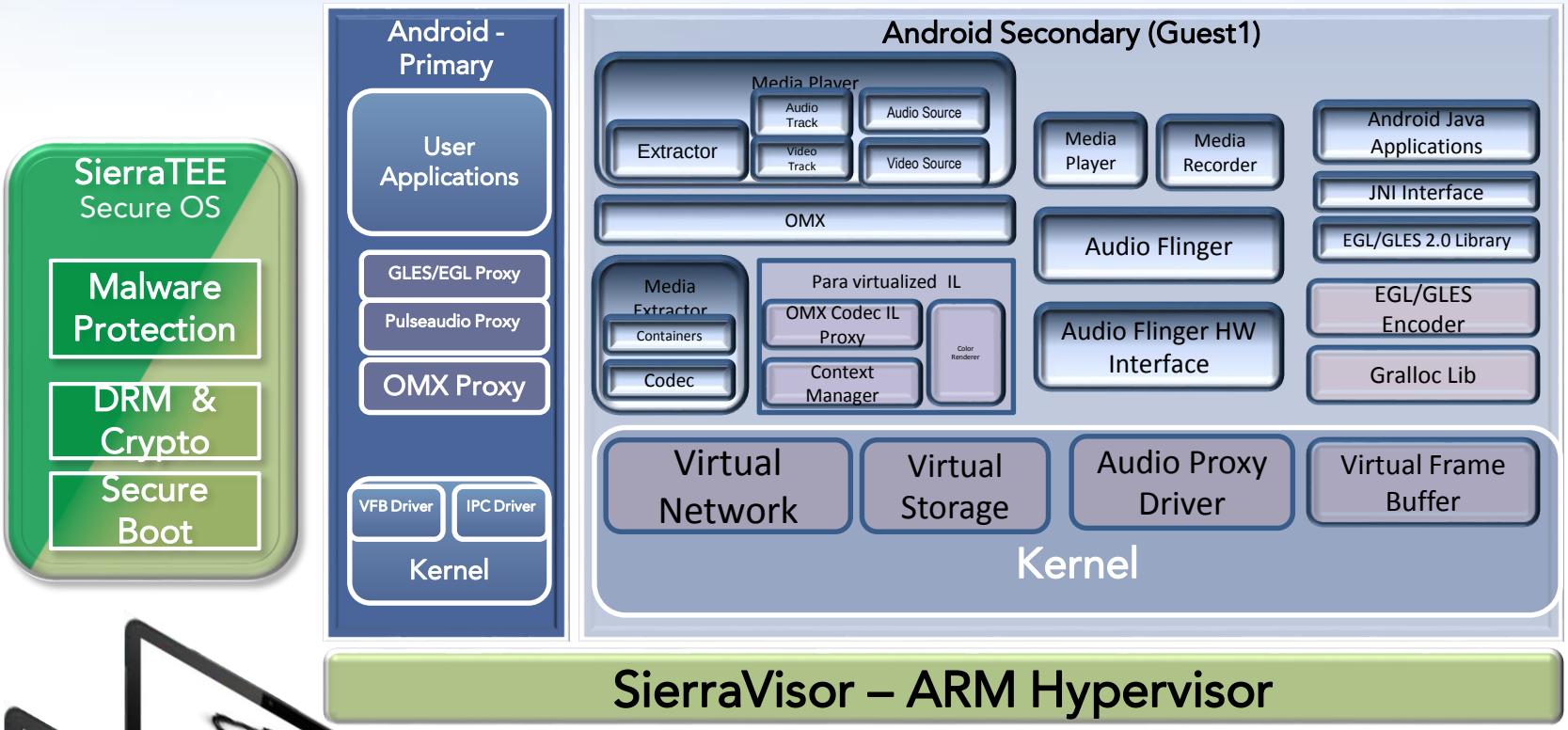
Simply Secure

Integration Challenges

- DRM Mandates TrustZone TEE
- Hypervisor provides the flexibility and security needed for BYOD
- Power management, responsibility spread across Multiple entities. TrustZone Monitor and Android Guests need co-operate.
- Efficient integration between TEE and Hypervisor is must to ensure seamless 1080p@60 video performance
- High performance GPU stack allowing for the ability to run un-modified apps on games.

sierraware

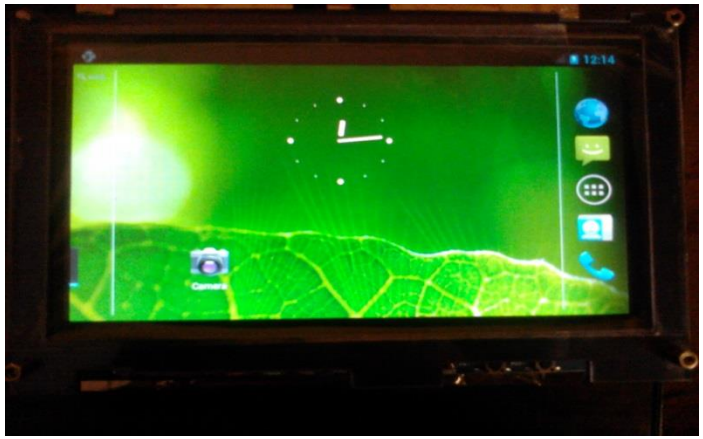
Dual Android



Android Work and Play. Bring Your Own Device to work

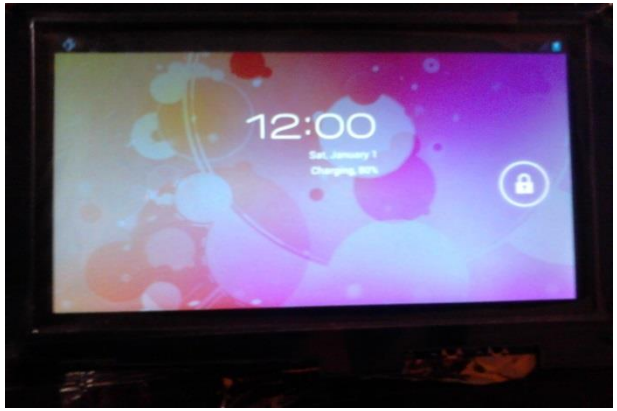
sierraware

Dual Persona Android



- Primary Android
- Full access to all the devices like Camera, LTE, SD Card
- Hypervisor overhead is below 0.5%
- Near native performance on GPU benchmarks and CPU benchmarks like Lmbench

- Secondary Android
- Virtual Network, Virtual Block
- Minimal changes to native Android stack
- Full GPU access; all games and apps can use GPU
- Gfxbenchmark with low overhead. Triangle, fill rate are near native performance.

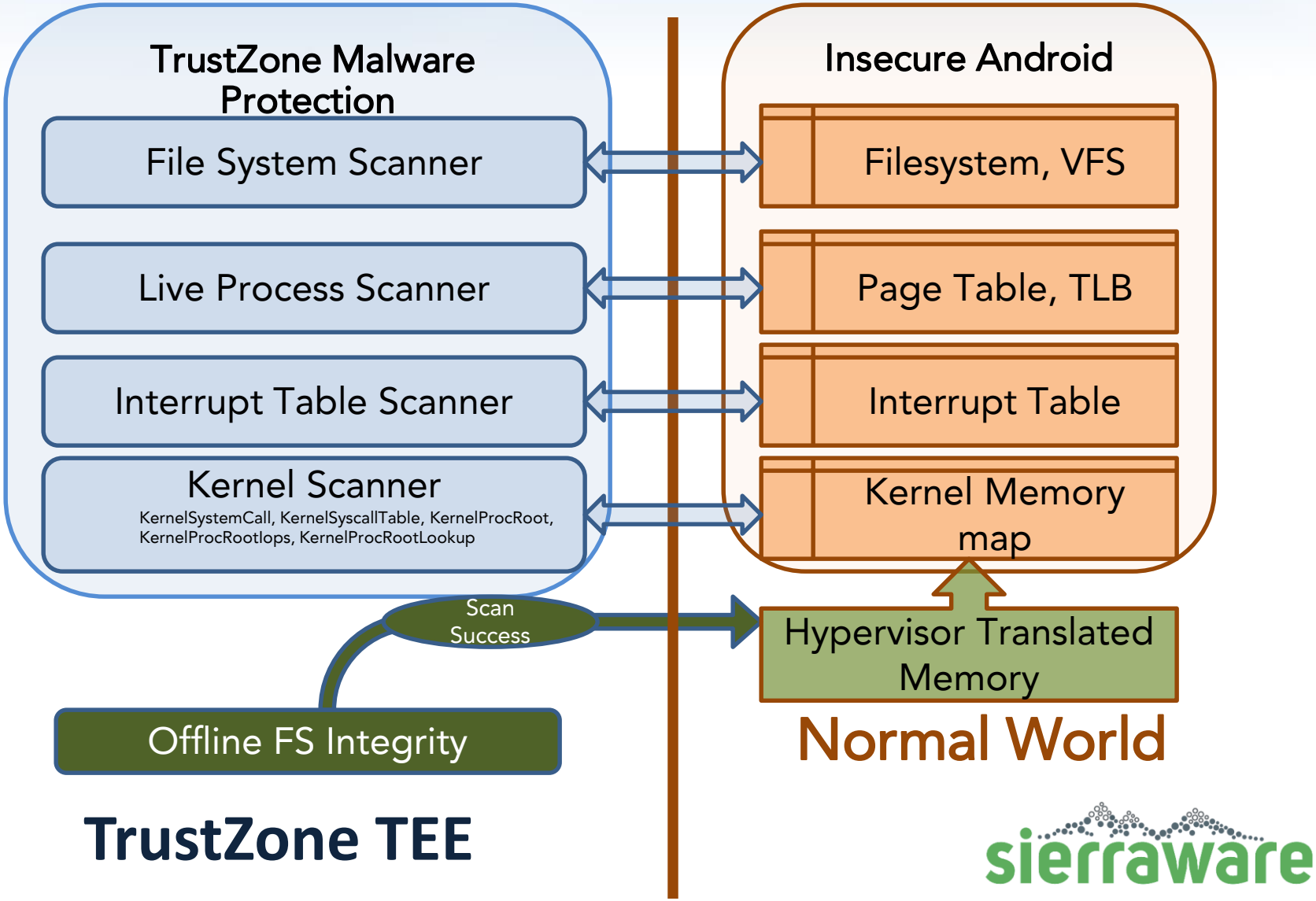


sierraware

Difficulties of Integrating TEE and Hypervisor

- TEE needs to be aware of 2 level memory translation
- Virtual Interrupts and VGIC are not directly visible for TEE
- Asynchronous task scheduling. Hypervisor scheduler needs to work with TEE scheduler to ensure one guest doesn't starve the other guest by residing in secure world for too long
- Global Platform APIs and SMC calling conventions were not designed with multiple guests and TEE domains

How to secure the devices from Malware ?



Difficulties of Integrating Android on a Hypervisor

- Linux Kernel is very conducive and been the most used guest operating system
- Android on the other hand is heavily tied to the hardware
  - Media Player
  - DRM
  - Power Management
  - Disk and I/O

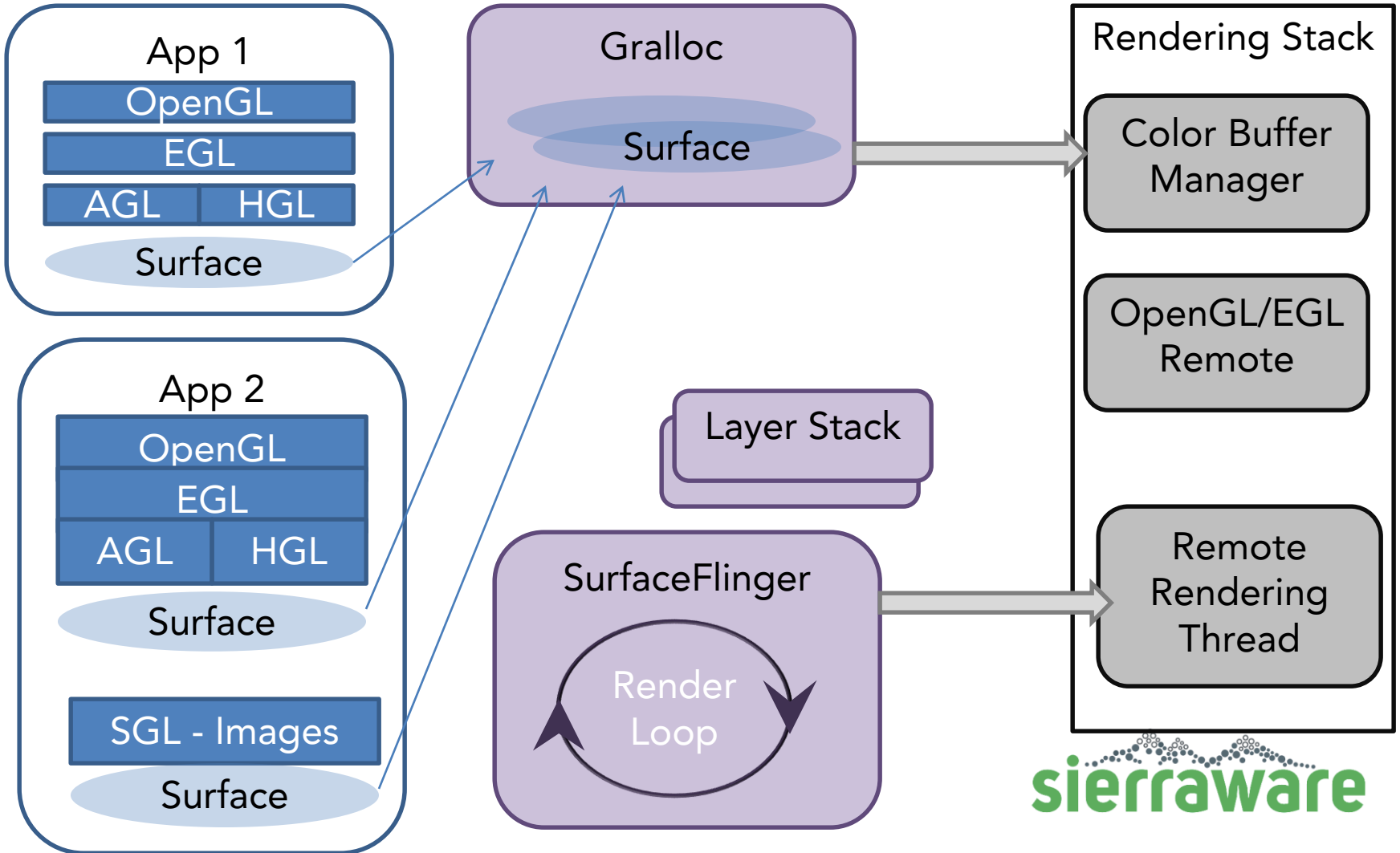
  and so many other things. Paravirtualizing all them and making sure they play well with TEE requires good pre-plan and well thought out design.

Integrating Remote GPU Rendering and Android

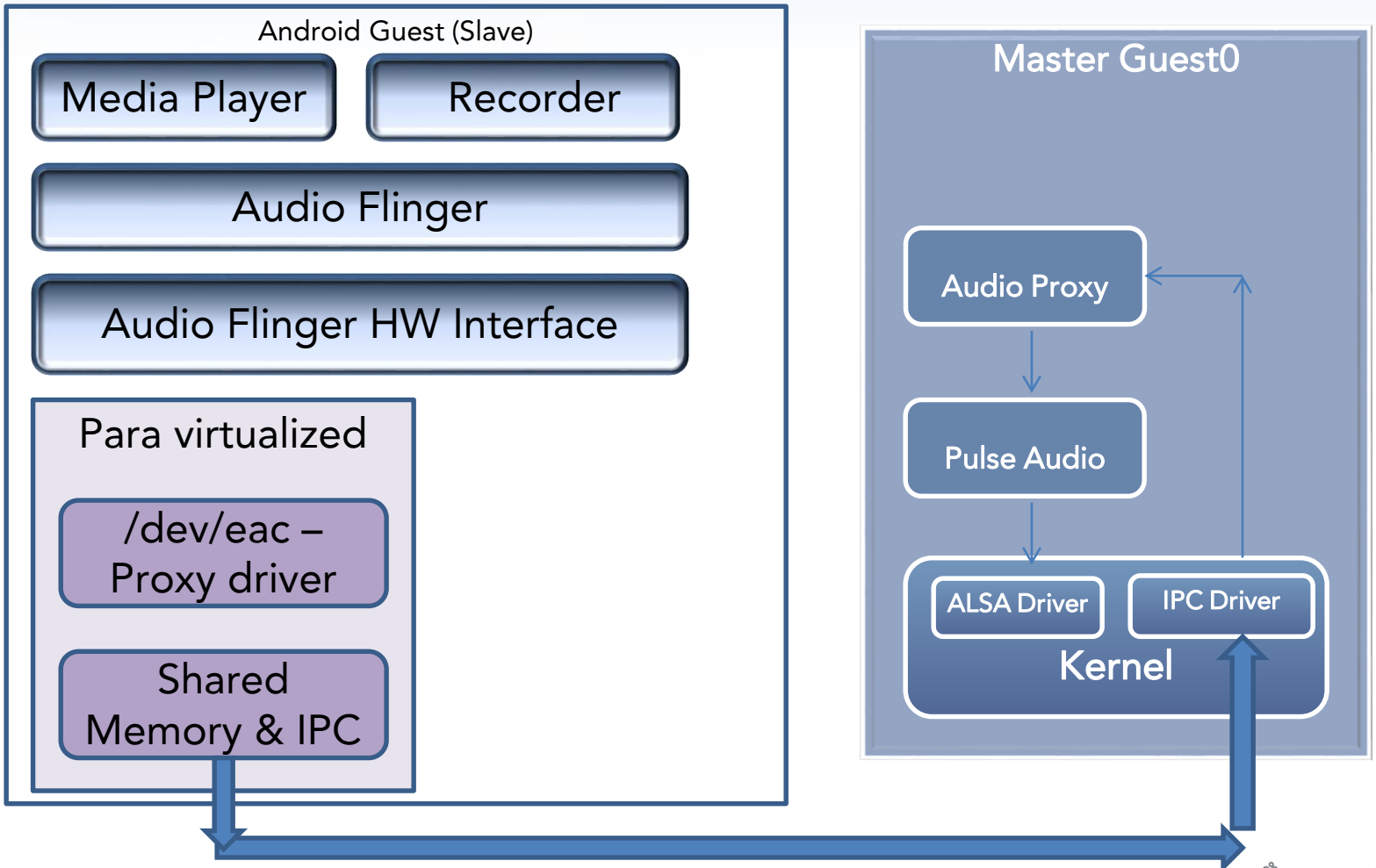
- Android is tightly integrated with OpenGLES & egl.
- Even simple things like cursor movement rely on Android GPU
- A 1080p frame is 7+MB of data. So moving 60 frames per second via para-virtualized drivers incurs huge cost penalty.

sierraware

GPU Rendering



Paravirtualizing Android Audio



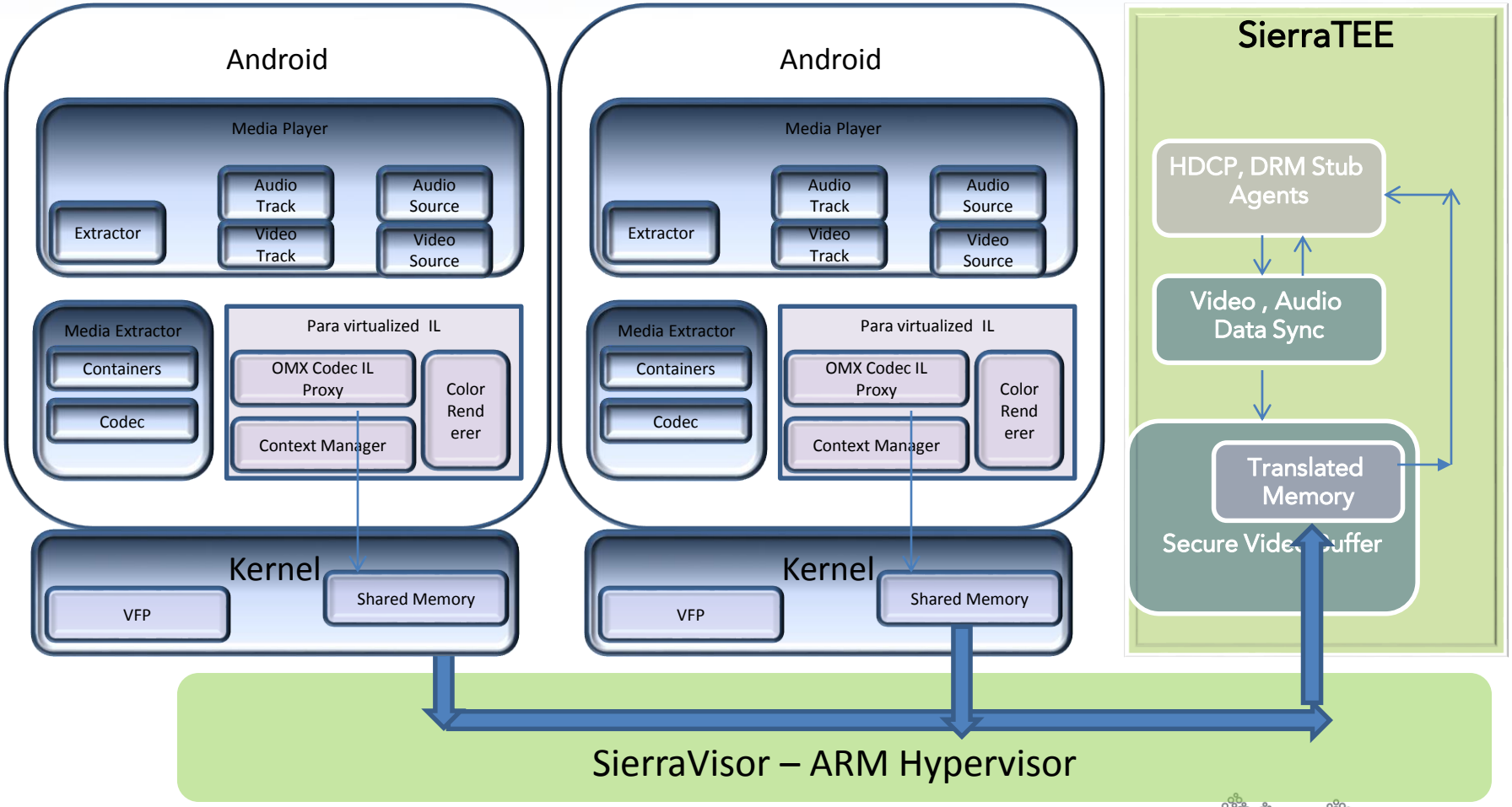
sierraware

DRM – Secure Video Data path

- DRM Mandates that both compressed and un-encrypted content must be kept out of guest memory space
- A Single Video Rendering path executed on TEE must serve multiple Guest OSes
- Physical memory translation between guest and TEE has to handled by a Integrated Solution
- Arbitration of resources is also important
- Ability to share hardware codecs and devices like speakers between multiple guests in a secure way is critical

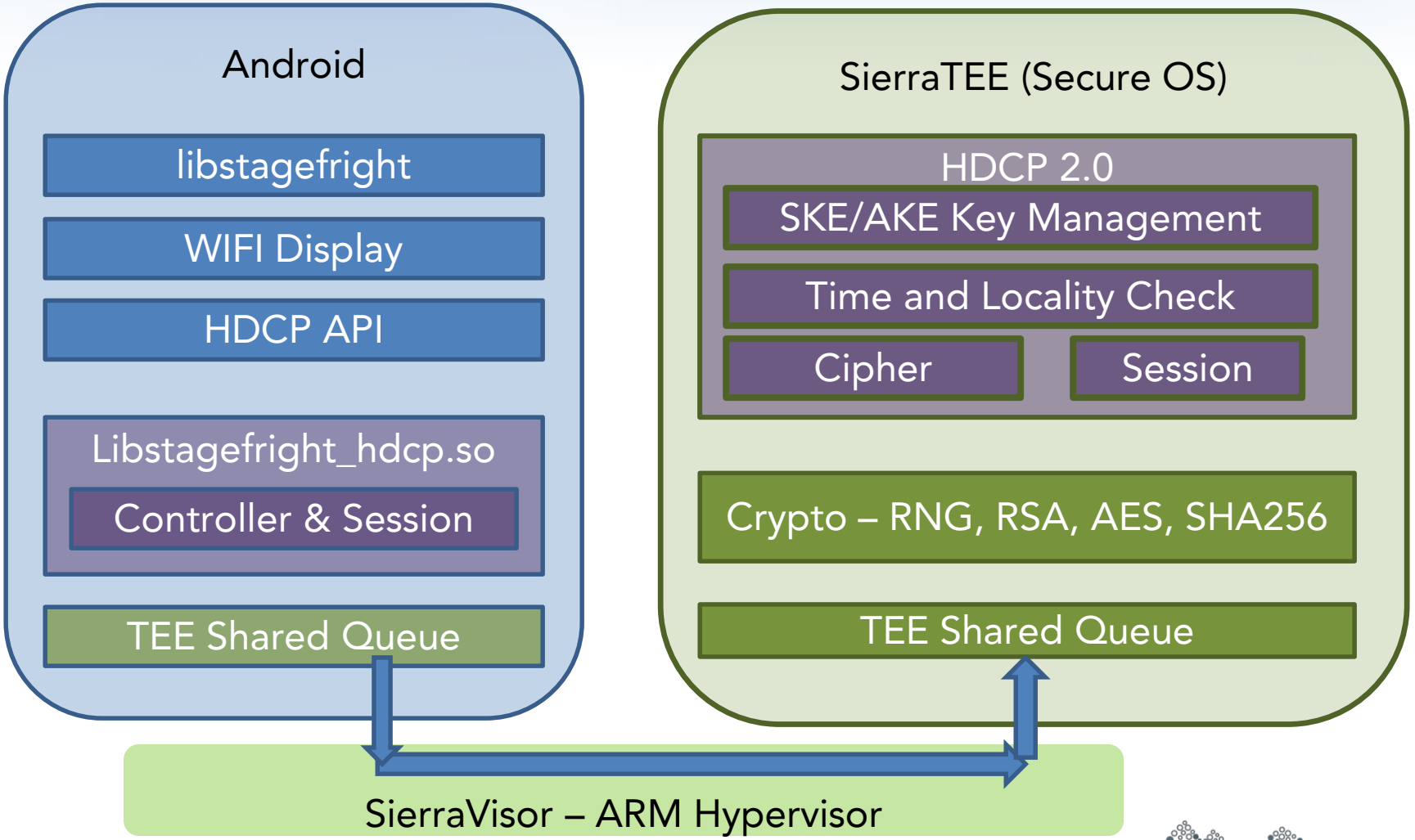
sierraware

DRM: TEE and Hypervisor



sierraware

Wireless Video/Miracast HDCP



sierraware

Other I/O Devices that needs to be para-virtualized

- Mouse/Keyboard/Touch screen
- USB, SDIO. External Storage
- Android Debugging and Shell
- Power Management like idle screen time out
- LTE, Telephony stack

sierraware

Virtio – Storage, Network, IPC

Para virtualized I/O: virtio provides an efficient abstraction for hypervisors and a common set of I/O APIs

Components of Virt I/O:

- Full support for SDIO, NAND, USB based storage devices
- RPMSG for IPC between guests. Provide high multi-gigabit performance.
- Virtual Network with Jumbo frame support. Ability to bridge Ethernet, WIFI, LTE and other network interfaces

sierraware

Support and Services

Simply Secure

Software Suite

- SierraVisor:
  - Hypervisor for ARM
  - Para-Virtualizaiton, TrustZone Virtualization, HW Virtualization
  - 64 bit Support for Cortex A5x cores
  - Linux, uCOS and various RTOS

- SierraTEE/Micro Kernel
  - TrustZone/GlobalPlatform TEE
  - Android, uCos and various other Oses
  - Runs on various CPUs from ARM11, Cortex A9, A15 and Cortex A53/57

- SierraSHIELD: Integrity Management
  - Linux Kernel Integrity Management
  - Application Rootkit Scanner
  - Incremental Log Scanner

- DRM and Content Protection :
  - Hardware accelerated media streaming and DTCP toolkit
  - Integration with Microsoft Playready

sierraware

Professional Services

Custom Services

- *Porting software to processors*
- Integrating TEE and SierraVisor with applications
- Developing drivers, encoders or apps

ARM Design Expertise

- Extensive experience with ARM processors and kernel code
- Android, Linux, BSD, and VxWorks development
- Hardware & FPGA

Project Management

- Phased approach from planning and development to testing & certification
- Carefully defined schedules and communication with customers to avoid surprises & delays

sierraware

Technical Support

- Telephone and Email Support
- Online technical documentation
- Software updates for commercial products
- Previews of upcoming releases
- Ability to influence feature enhancements
- Commitment to Quality
  - Service Level Agreement (SLA) details support response times and escalation levels

sierraware

Thank You!

sales@sierraware.com, +1 408 337 6400