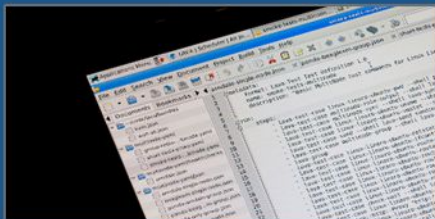


# 让应用之花开在最佳的“土壤”之上

## - Linaro安全方案的最新现状和计划

严念 (Leo Yan)

Linaro Premium Service



# 日程

- Linaro和安全工作组简介
- 最新的解决方案
- 后续的计划

核心会员  
(Core)

ARM®

 **HISILICON**

 **QUALCOMM  
INNOVATION  
CENTER, INC.  
QuIC**

俱乐部会员  
(CLUB)

 **MEDIATEK**  
*everyday genius*

 **TEXAS  
INSTRUMENTS**

**socionext™**  
for better quality of experience

 **SPREADTRUM®**

  
*life.augmented*

**ZTE中兴**

组会员  
(GROUP)

  
**Alibaba Group**

 **炬力  
Actions**

 **Allwinner  
Technology**

**AMD** 

 **apm applied  
micro**

  
**BROADCOM®**

 **CAVIUM**

  
**CISCO**

 **MEIZU 魅族**

 **CITRIX®**

  
**COMCAST**

  
**ENEA**

  
**ERICSSON**

  
**facebook**

  
**freescale™  
semiconductor**

  
**hp**

  
**Mstar  
semiconductor**

  
**MARVELL®**

  
**MontaVista**

**NOKIA**

  
**Google**  
学术搜索



**redhat.**

  
**WIND™**

社区会员  
(COMMUNITY)

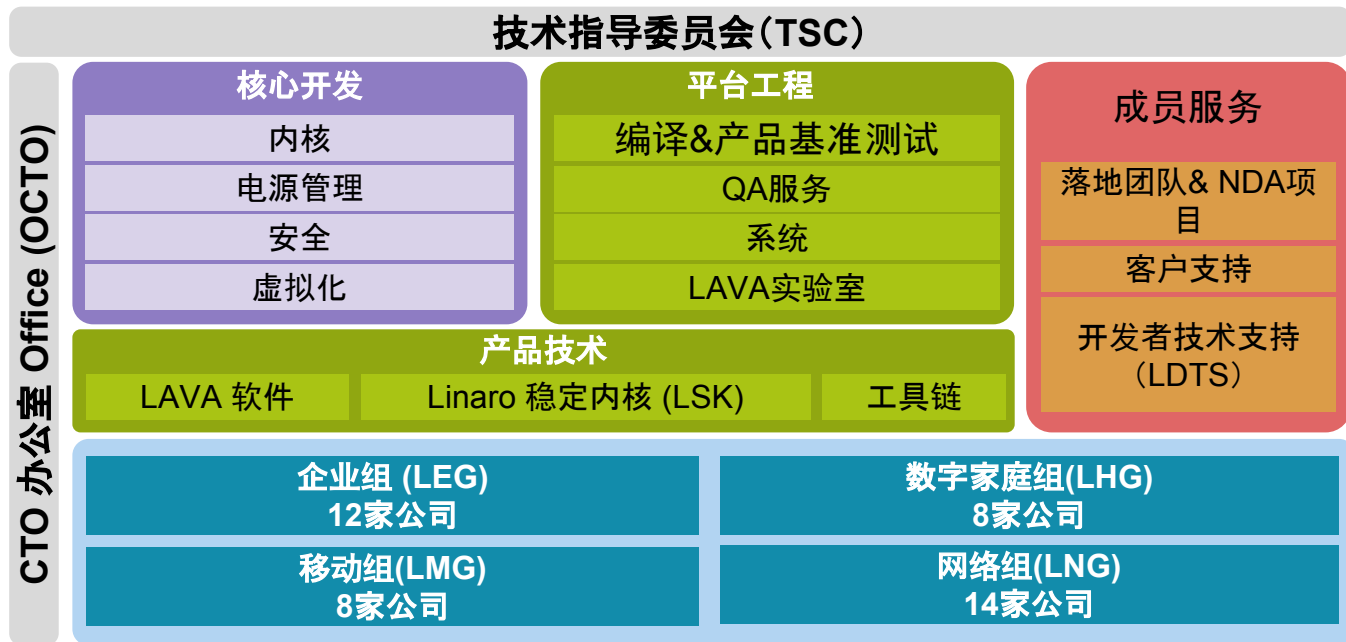
  
**IBM®**

  
**THE  
LINUX  
FOUNDATION**

  
**Linaro**

# Linaro组织

- 于2010年由6个会员一同创立，如今拥有38名会员
- 公司在全球约有230名工程师



# Linaro 工作组介绍

## 数字家庭组-LHG



### 数字家庭组开源软件

- 适用于RDK和安卓的W3C EME安全媒体回放
- 中间件和用户空间堆栈
- DRM, DLNA, CVP-2, HTML5
- 适用于STB/IPTV的LSK内核
- 通用媒体框架

## 移动组-LMG



### 移动组开源软件

- 安卓64位, L 版本
- big.LITTLE电源管理
- QEMU开发
- 64位Chromium浏览器
- 支持成员, ARM和谷歌的安卓开发

## 网络组-LNG



### 网络组开源软件

- 实时支持
- 虚拟化
- 核心隔离
- OpenDataPlane (ODP)
- 大字节序遗留系统支持
- 片上系统加速器的ODP跨平台支持

## 企业组-LEG



### ARM服务器开源软件

- UEFI/ACPI
- KVM/Xen
- ARMv8优化
- OpenJDK, Hadoop, OpenStack
- 减少碎片化、降低成本并使产品加速投入市场

# Linux内核代码贡献量

- Linux 内核 3.11 - 3.18
- 2013年9月-2014年11月
  - 这些发布中包含超过96000个总变更集
- 已知有518家公司参与到项目中来
- Linaro贡献率位列第三

Top Linux Contributors by Company: 内核s 3.11-3.18  
Linux公司贡献值排行榜

|    |               |                     |
|----|---------------|---------------------|
| 1  | None (个人开发者)  | 11,968 (12.4%)      |
| 2  | Intel         | 10,108 (10.5%)      |
| 3  | Red Hat       | 8,078 (8.4%)        |
| 4  | <b>Linaro</b> | <b>5,415 (5.6%)</b> |
| 5  | Samsung       | 4,290 (4.4%)        |
| 6  | Unknown       | 3,842 (4.0%)        |
| 7  | IBM           | 3,081 (3.2%)        |
| 8  | SUSE          | 2,980 (3.0%)        |
| 9  | Consultants   | 2,451 (2.5%)        |
| 10 | TI            | 2,269 (2.4%)        |

# 96Boards 开源硬件规格

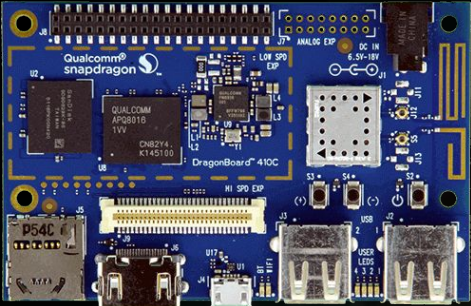
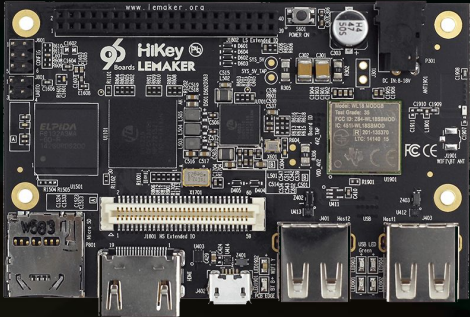


- ▣ 价格: ~\$50-150
- ▣ 用于智能手机/嵌入式设备 SoCs
- ▣ 面向软件开发者、创客、研究机构、大学和OEM



- ▣ 价格: ~\$300
- ▣ 用于服务器/网络设备 SoCs
- ▣ 面向软件开发者、大学&研究机构、SoC评测和测试/编译农场(build farms)

# 已发布96板

|      |                                                                                   |                                                                                     |
|------|-----------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
|      |  |  |
| Name | DragonBoard 410c                                                                  | HiKey                                                                               |
| CPU  | 高通SnapDragon™ 400<br>4核Cortex-A53                                                 | 海思麒麟 6220<br>8核Cortex-A53                                                           |
| GPU  | Adreno 306                                                                        | Mali 450-MP4                                                                        |

其它: 炬力Actions Semi (CE), Arrow/Freescale i.MX7 (CE) 和 AMD (EE)  
未来6个月还会发布更多其它96板

[www.96Boards.org/products](http://www.96Boards.org/products)

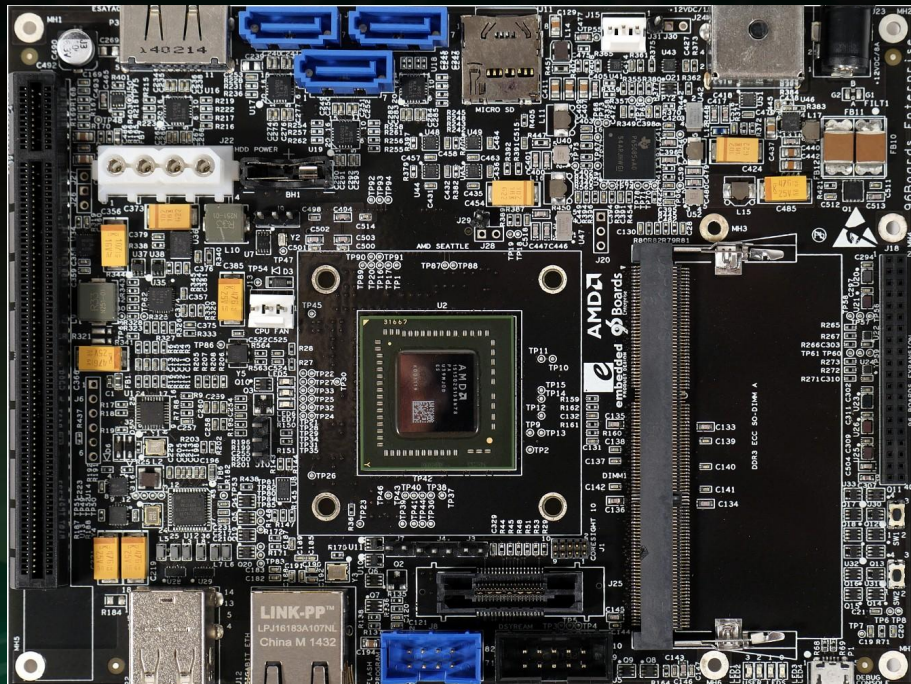
HiKey 可以在EL3/S-EL1模式下运行代码, 可用于开发安全软件

96Boards

# 96Boards 企业级版 (EE)

即将发布！

- AMD HuskyBoard
  - 96Boards EE
  - 四核 Cortex-A57
  - 千兆以太网口
  - SATA/eSATA
  - x16 PCIe G3
  - SO-DIMMs up to 16GB



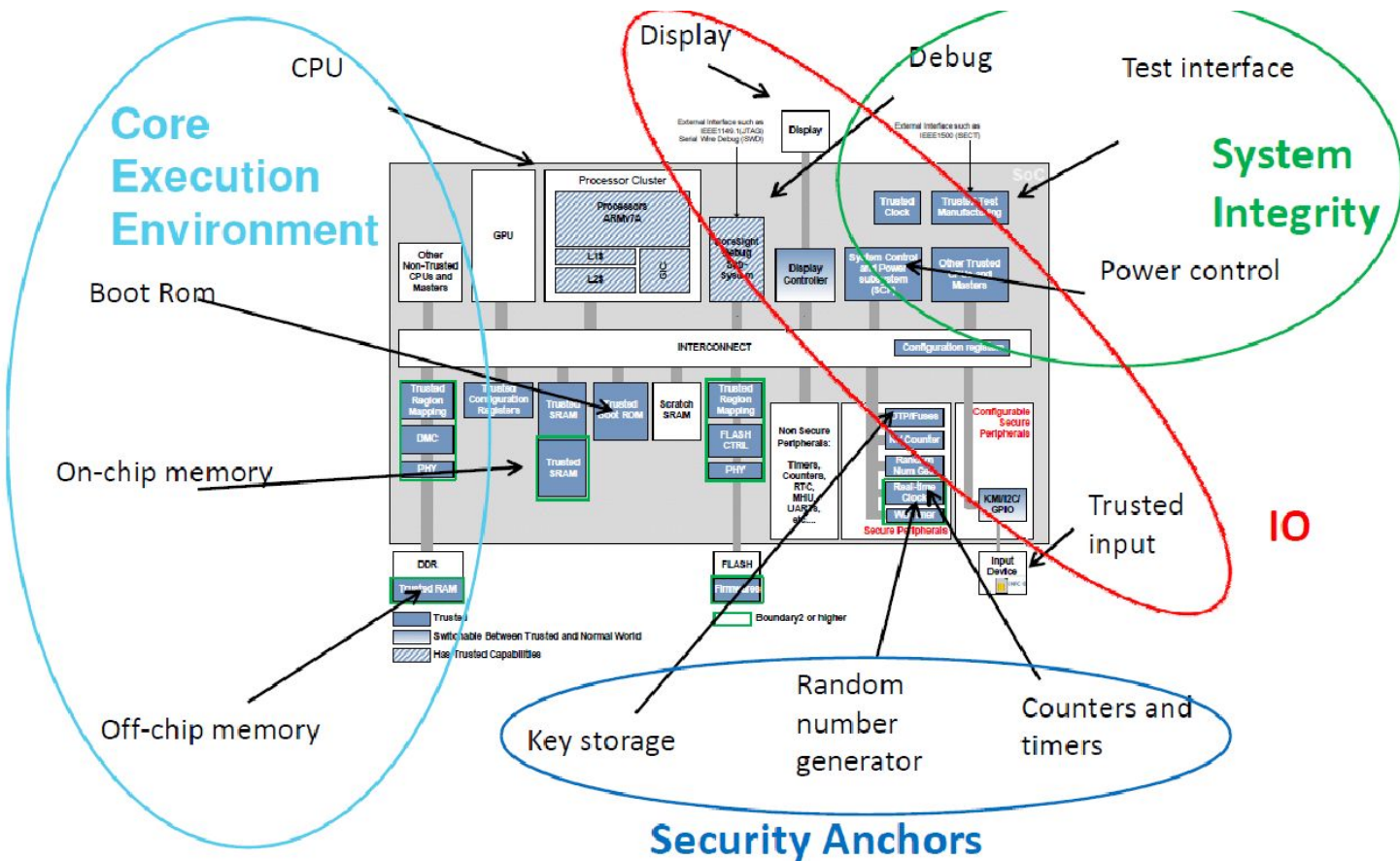
# Linaro安全工作组

- 成立于2013年10月
  - 主要目标: 开源的TEE解决方案和对于内核的安全保护
  - 整合ARM社区的软件解决方案和防止碎片化
- 项目组
  - 技术Leader: Joakim Bech
- 专注的技术
  - TEE / TrustZone
  - 安全启动 (ARM Trusted Firmware, UEFI and U-Boot)
  - 数字版权管理
  - 内核的安全保护

# 日程

- Linaro和安全工作组简介
- 最新的解决方案
- 后续的计划

# ARM SoC的硬件架构



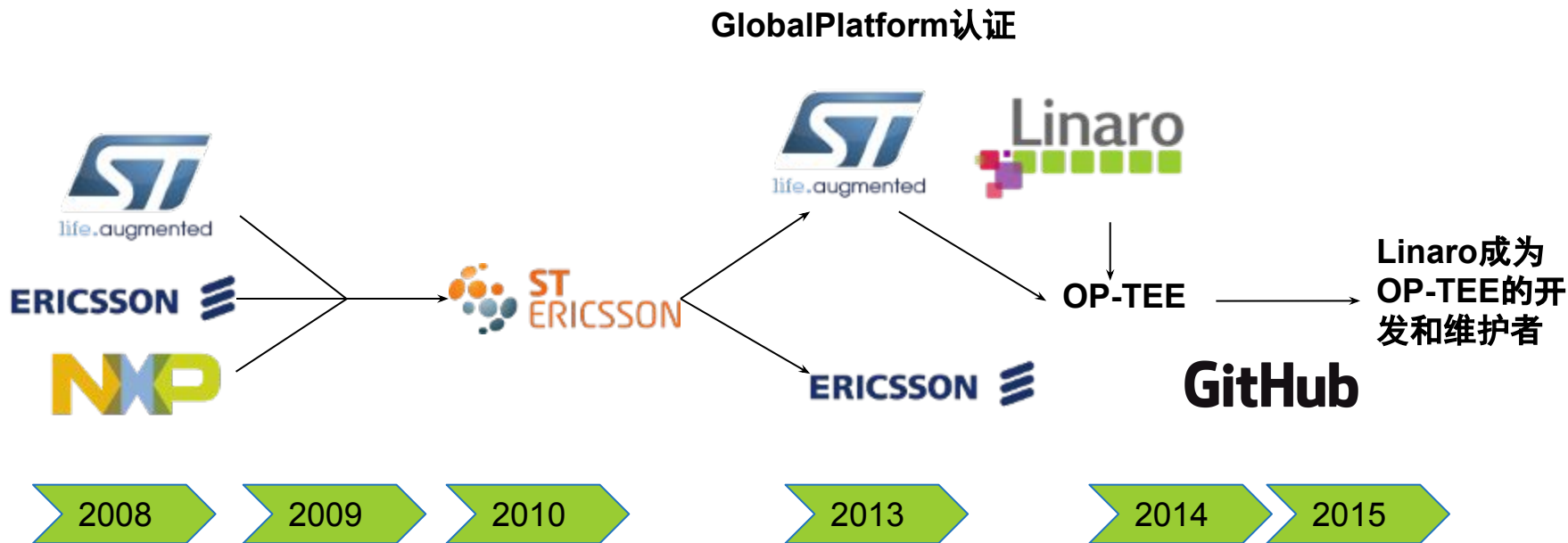
# 安全软件方案需要考虑的问题

- 硬件的加解密驱动
- 安全启动
- 密钥的管理
- 硬件上不同的安全属性的管理
  - CPU: 基于ARM TrustZone, 分为了安全空间和非安全空间(World)
  - 内存和总线: 安全内存, 安全的总线端口
  - IO: 安全显示, 安全输入, 安全存储
  - DMA控制器, 中断的响应, 定时器, watchdog, etc
- TEE是安全运行环境的基础框架

# 如果我们没有统一的TEE软件方案？

- GlobalPlatform定义了TEE的规范
  - 但是SoC厂商和OEM需要开发自己的TEE方案, 所以引入了很多的碎片化和兼容性的问题
- 实现TEE的技术难点
  - 安全空间和非安全空间有自己的OS, 每个OS需要开发内核驱动, 中间件, 上层应用; 还需要完整的测试框架和测试用例用于验证
  - 设计上的难点: 两个空间的中断处理, 内存空间的隔离, 消息通道的实现, 如何减少代码的占用空间, 性能的调优 (例如共享内存), 电源管理等
  - 需要花费较长的人力和时间才能够产品化

# Open Portable TEE (OP-TEE)的路线图



# OP-TEE概述和依从的API

- 在ARM社区里有效的防止碎片化和整合统一的方案
- 支持ARMv7-A (32比特)和ARMv8-A (64/32比特)
- 可以进行软件模拟(FVP和QEMU)
- 依从于GP Client API (v1.0)
- 依从于GP Internal API (Core v1.1)
- 依从于GP Secure Elements (v1.0)
- 支持安全启动的架构和Secure Video Path

# OP-TEE现有成果

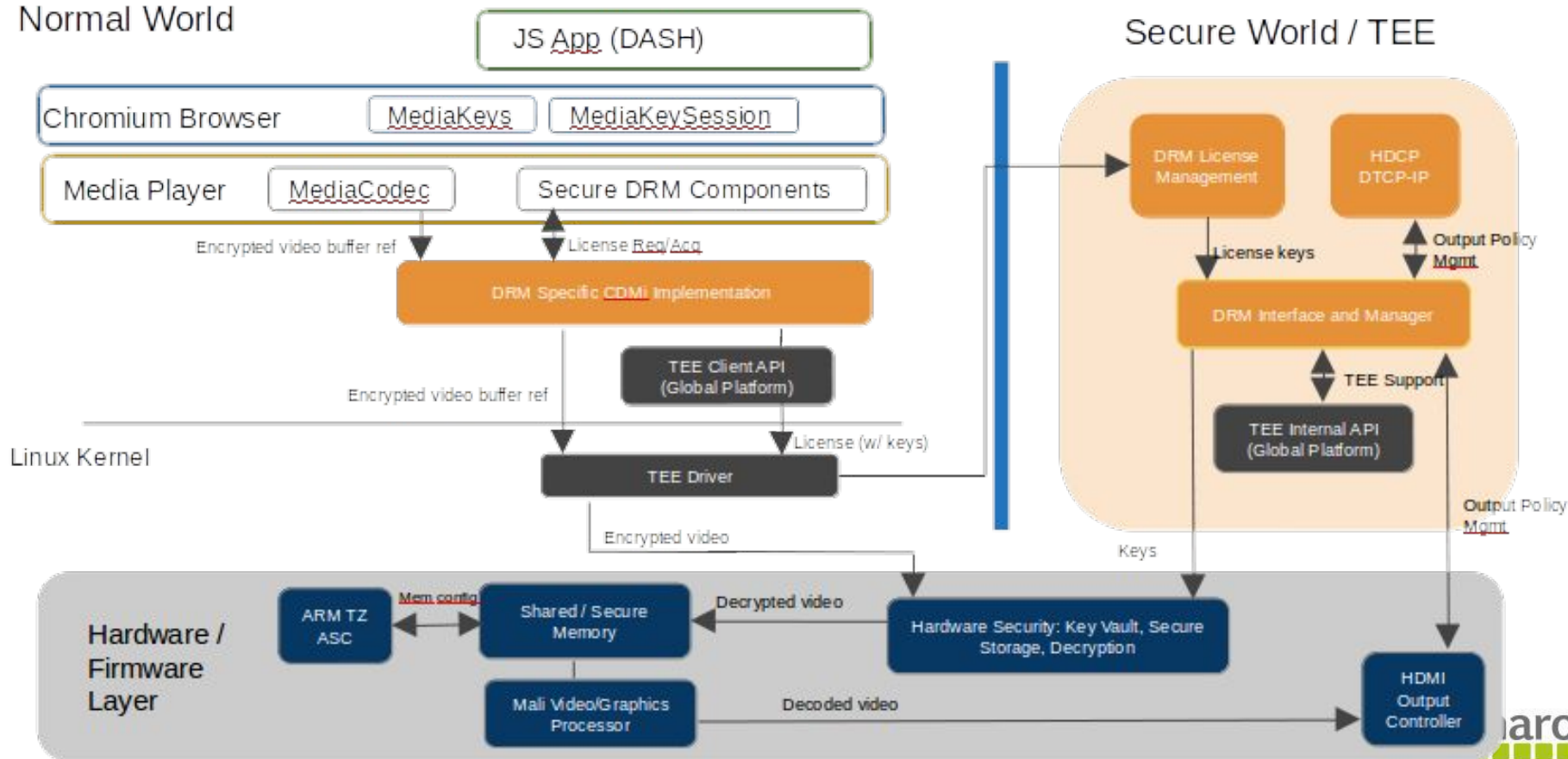
- 对运行空间进行了优化(200~300KB)
- 静态和动态的加载安全应用程序(TA)
- 基于Rich OS(Linux kernel)的调度策略
- 基于功能的消息机制
- 基于RPC的消息机制
- Pager: 充分利用DRAM和加强安全性
- 支持加解密库LibTomCrypt
- 支持在两个空间中共享内存
- 测试框架:xtest

# ARM Trusted Firmware

- OP-TEE需要和ARM Trusted Firmware一起工作
  - 对于IRQ / FIQ的使用
  - OP-TEE dispatcher已经合进ARM-TF
- ARM-TF实现了安全启动
  - 信任的根节点: BootROM (BL1) + Root key
  - 对密钥和内容的认证

# 基于OP-TEE的数字版权管理方案

Normal World



# 不同的数字版权管理方案的集成

- 由Linaro数字媒体工作组开发 Digital Home Group (LHG)
- 集成Google Windwine
  - 使用Chromium浏览器
  - 依从于W3C EME规范
  - 使用Open Content Decryption Module interface (OCDMi)作为标准接口
- 对Microsoft PlayReady DRM进行概念上的验证
  - The PlayReady porting kit v3 在架构上是提供了对于TEE的接口
  - 实现了在安全空间里面DRM应用程序
  - 已经在硬件上完成基本原型的验证工作

# 日程

- Linaro和安全工作组简介
- 最新的解决方案
- 后续的计划

# OP-TEE的工作计划

- 提交OP-TEE's Linux内核驱动的patch
- 加强对安全存储的实现
- 实现对RPMB (和RPMB模拟器)的支持
- 实现对GP Test suite v1.1的支持
- 将OP-TEE的Linux内核驱动移植到Linaro Stable Kernel
- 支持SPI总线的支持, 从而可以支持安全显示

# DRM进一步的集成和整合

- 继续对Google和Microsoft两大生态系统的支持
  - 软件方案的完善
  - 开发工具组件的完善
- 与广电总局TVOS的合作
  - 2015年12月26日: Linaro和广电总局TVOS WG宣布合作; Linaro加入TVOS工作组 (60多个会员), TVOS工作组同时也加入Linaro LHG (9个会员)
  - 基于OP-TEE, 会帮助TVOS作为主要TV/STB的开放平台进行推广
  - Linaro LHG会集成TVOS的ChinaDRM的实现框架
  - Linaro中国区的会员(例如Huawei, Alibaba, ZTE等)可以从合作中受益



More about Linaro: [www.linaro.org/about/](http://www.linaro.org/about/)  
Linaro members: [www.linaro.org/members](http://www.linaro.org/members)