ARM TrustZone 安全技术培训

摘要：
本课程旨在向平台开发人员完整地概述如何使用 ARM TrustZone 安全技术设计可信系统。

课程将介绍 v8-A 架构的特权模式和内存隔离特性。另外还介绍安全启动、DRM 或移动支付等应用示例对平台和软件的需求。课程将讨论完整的可信系统，包括：
- 安全启动
- 安全监控
- 可信内核和可信应用
- 普通模式下的安全驱动
- 正常模式的应用程序开发
- 平台设计
- 内存保护

参与培训的必备条件：
- 具有 ARM 应用处理器的实际设计经验
- 了解 C 语言编程
- 具有汇编程序编程的经验会非常有用，但并不是绝对必要
- 具备嵌入式系统的基本知识

受众：
面向需要了解在使用 ARM TrustZone 安全技术扩展开发可信系统时出现问题的软硬件系统架构师。

课程培训天数：
3 天

课程内容：
- ARM 架构简介
- Aarch32 架构基础知识（可选）
- TrustZone 简介
- TrustZone 硬件概述
- TrustZone 软件概述
- TrustZone 内存管理
- TrustZone 异常处理
- 虚拟化
- 系统构造软件指南
- SMMU 编程（可选）
- TrustZone 安全启动
- TBBR 和可信固件
- TrustZone 系统架构
- TrustZone 软件栈
- TrustZone 安全调试
- TrustZone 生态系统