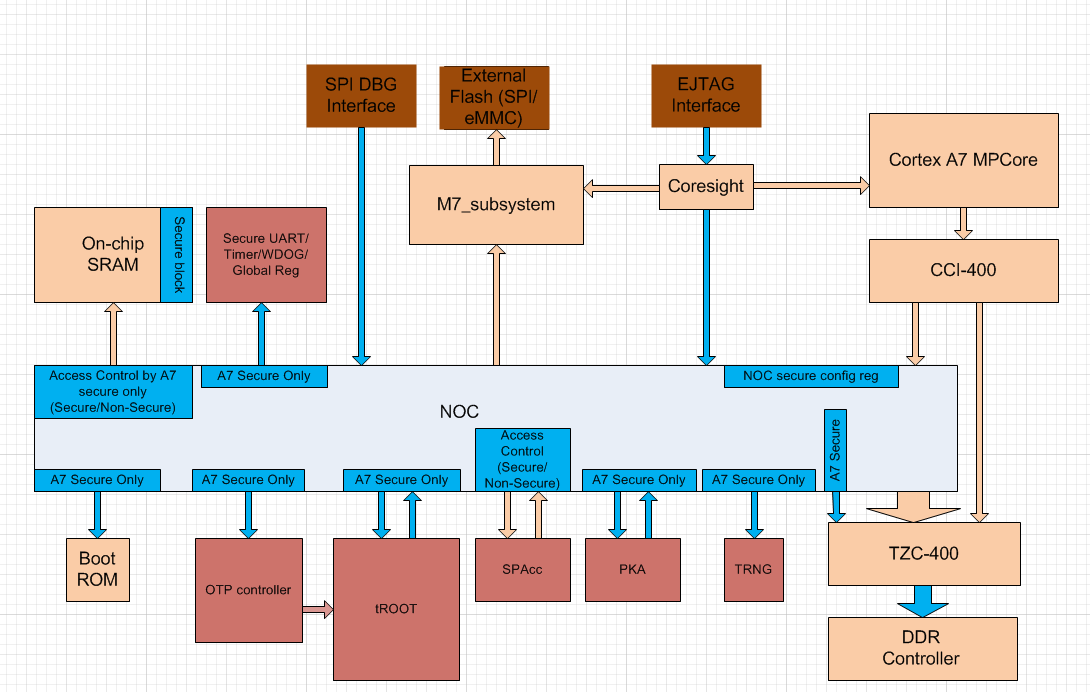
# 安全子系统

# 简介

基于最先进的ARM Cortex A7多核CPU trustzone技术的TEE（可信执行环境），整合了Synopsys的安全处理器tRoot, 结合自身芯片整体结构，提出了一套完整的安全子系统，对于芯片的关键模块进行保护，如密钥管理，版本控制，库函数保护，数字内容加密，安全升级，安全存储，安全启动,防止边带攻击等，防止任何不授信的软件攻击，获取视频、数据、应用软件信息等，从而使芯片处于安全系统控制中。

# 框图



安全子系统SoC结构图

# 性能

* 支持ARM v7-A架构的trustzone安全技术，包括了Cortex A7多核处理器，CCI-400，SMMU，TZC400等硬件核心部件，通过安全操作系统和非安全操作系统的隔离，在物理上防止系统攻破后关键数据泄密。
* 支持从tRoot经过验签后的安全加密授信image 文件启动。
* 支持硬件模式AES 256/192/128 ，DES 加密算法，支持加密模式 ECB/CBC/CTR/OFB/CFB/F8/XTS/CCM/GCM。
* 支持硬件模式hash 加密算法，MD5/SHA-1/SHA-256/SHA-512/SHA-512/256。
* 支持软件模式RSA 最大4096bit， ECC 最大512bit 加密算法。
* 支持从内部8KB安全ROM加SPI NOR flash 或者加eMMC NAND flash的系统启动方式，以及系统安全升级，数据安全存储和系统安全debug。
* 内置128Kbit OTP内存，进行Root key和密钥保护，硬件信息，版本控制信息，库信息等安全存储。
* 内建基于ring-oscilloator的种子发生器的正随机数发生器，产生随机数用于安全系统管理。
* 内建可以配置的最大2MByte大小的安全SRAM，用于安全操作系统运行和安全数据的存储。