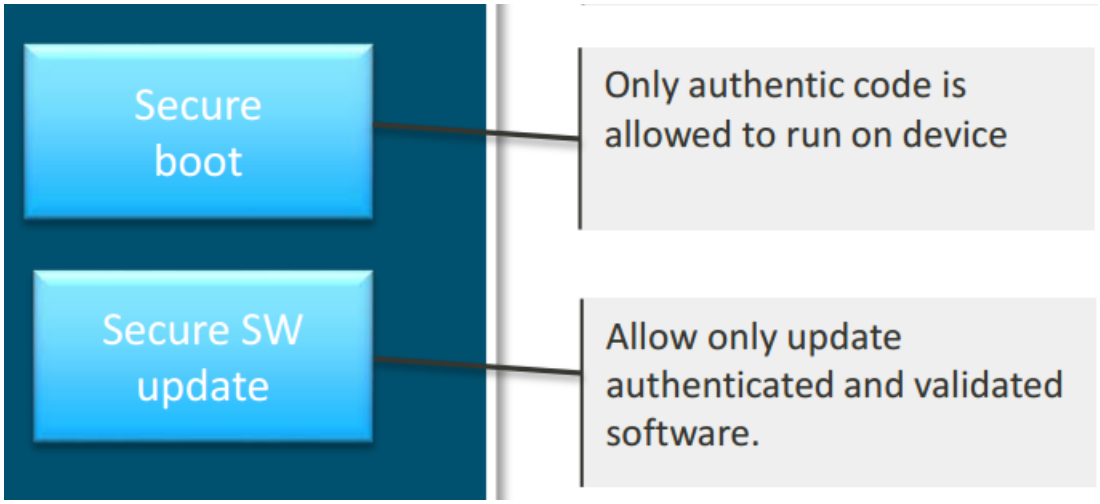
一、 固件安全升级说明

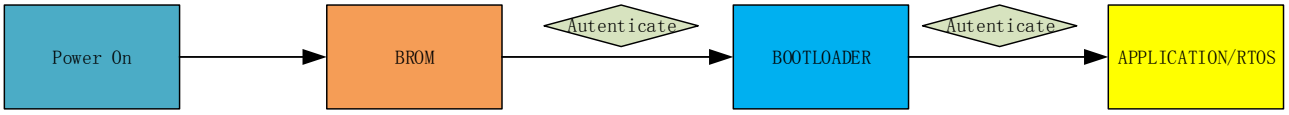
模组基于 MTK2625 平台开发，单核 CORTEX-M4 ，主频 104MHZ ，模组支持 security boot 和安全下载机制，保证运行固件的合法性和完整性：



固件列表

IMAGE	Attributes
BROM BIN	Read-only， Trust BIN
Bootloader BIN	Authenticated by BROM
APPLICATION BIN	Authenticated by BOOTLOADER

系统启动流程：



1. 开机，按照 CMSYS spec 的描述，CM4 core 会先执行 BROM 的代码，地址为 0x04100000.
2. BROM 会将 bootloader bin copy 到 RAM 中，先进行签名校验，校验通过跳转到 bootloader 代码执行
3. BOOTLOADER 会对 APP BIN 先进行签名校验，校验通过跳转到 APP 代码执行

   NOTE:

   (1) BROM 代码是一段固化代码，后续无法修改

   (2) 使用 RSASSA-PSS 签名算法和 SHA256 哈希算法

   (3) public key 会存放到 FLASH，防止 public key 被篡改，将 public key 的 SHA256 HASH digest 存放到 efuse Trusted FW 会校验 public key 的完整性

   (4) 下载工具可以做到永久无法读写 FLASH, Disable Flashtool

   (5) MTK 提供签名工具用于对 bootloader 和 app bin 进行签名

   (6) MTK 提供 KEY 生成工具用于生成 RSA key 和 public key hash

二、 Secure FOTA

1. 使用 FOTA packaging tool 生成签名的升级包
2. 将已经签名的升级包上传到 server
3. 模组开机使用 FOTA 的 AT 命令触发升级
4. 下载升级包到本地
5. 签名校验成功，重启进入 Bootloader，开始版本 updating
6. 如果签名校验失败，不执行任何的升级流程