Connecting the World !

Winner Micro

联盛德微电子固件防拷贝方案

www.winnermicro.com

概述

固件安全防拷贝方案是基于联盛德Wi-Fi/蓝牙Combo的W800系列 SoC实现，主要涉及如下几方面技术：

- 安全启动

  ROM支持芯片安全启动，采用硬件验签算法

- 固件加密

  支持运行加密固件，采用RSA保证了加密密钥的安全

- 防拷贝

  可提供芯片唯一序列号

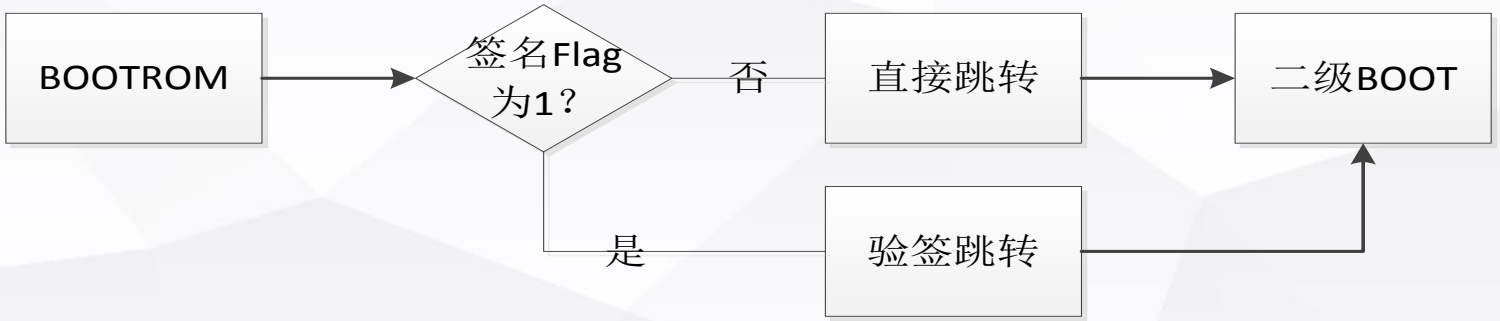
- 适用型号

  W800、W801、W805、W806、W861

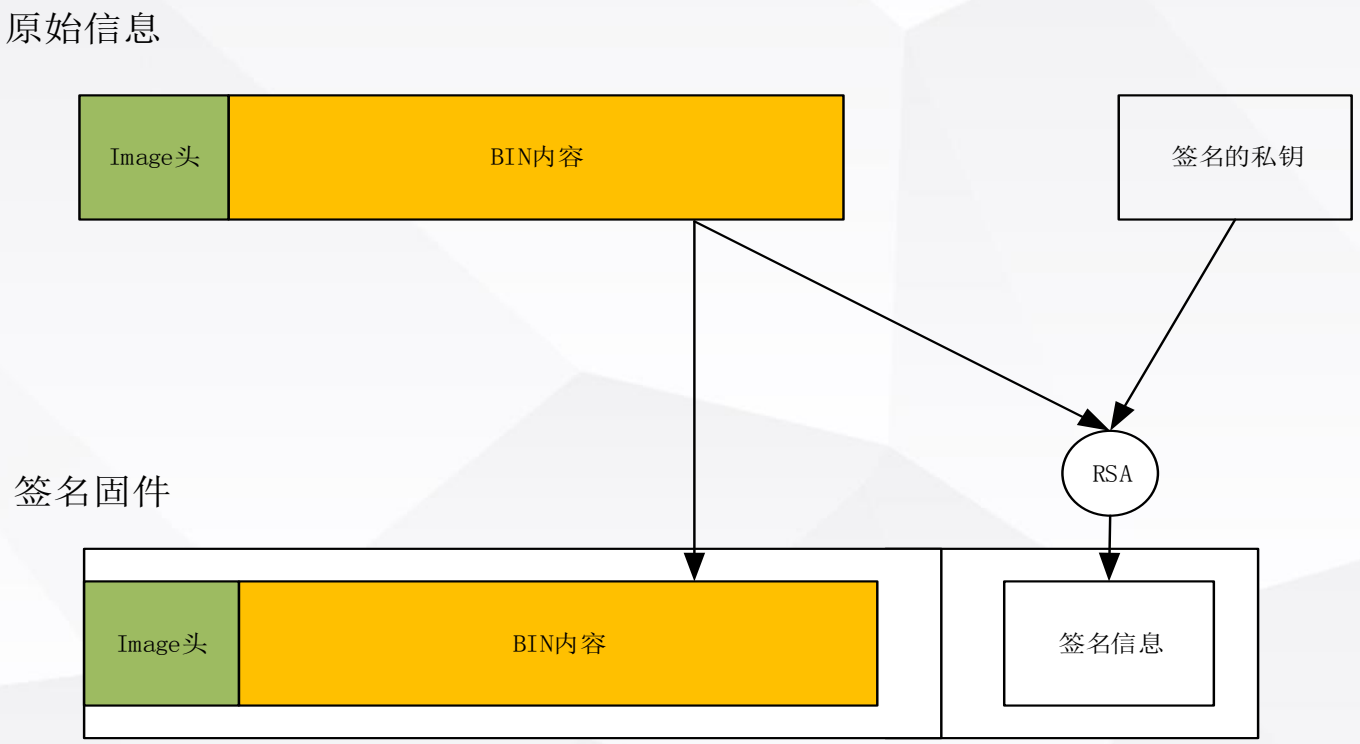
安全启动

W800芯片内置ROM，作为芯片的固定启动位置。ROM中的启动代码不可修改，并且支持了对二级BOOT的签名验证，验证过程由W800芯片内置的硬件加密模块进行加速，保证了启动的快速性。

签名标志存放位置：OTP区域，可加锁



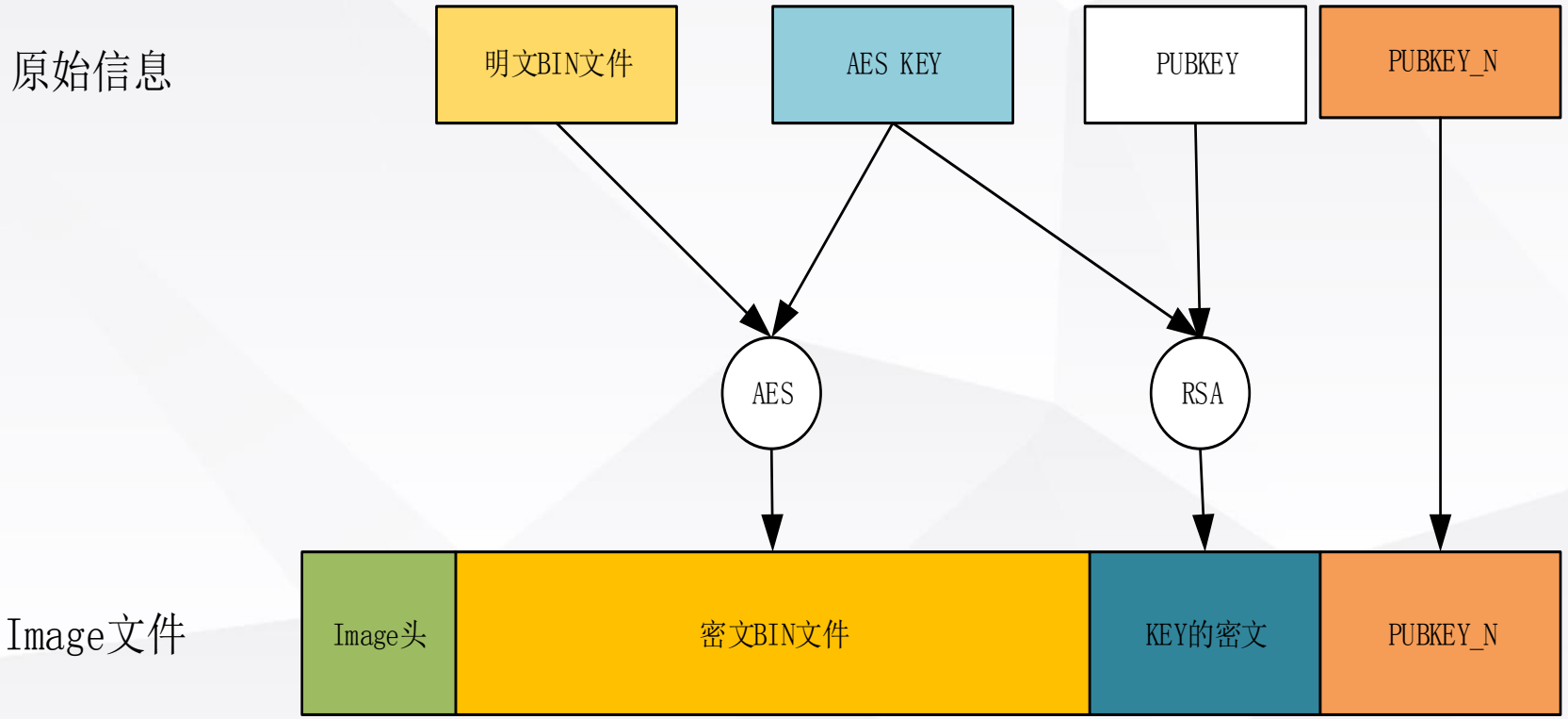
签名固件的生成



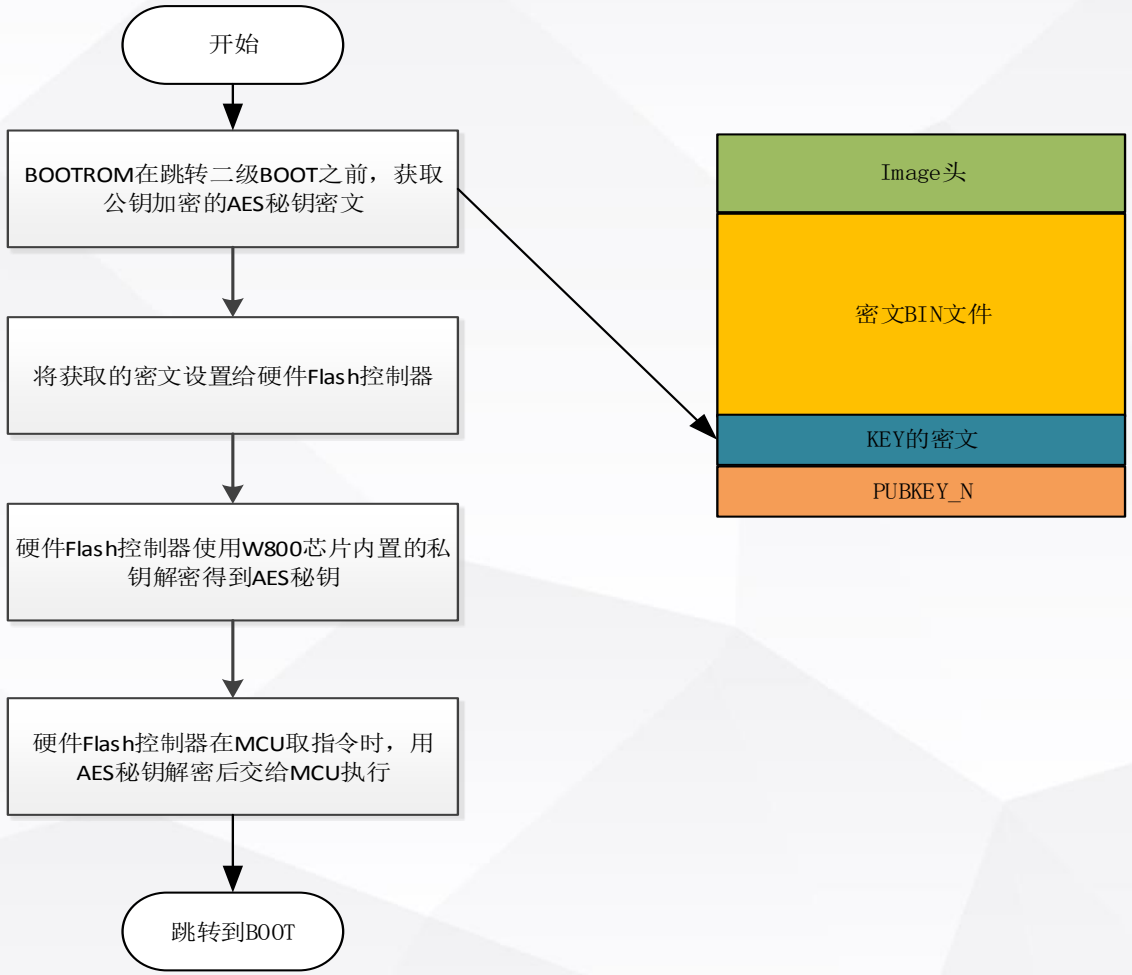
加密固件

- W800芯片支持运行加密的Flash固件
- 采用AES 128的对称加密算法
- 采用RSA对加密key进行保护
- 硬件解密运行

加密固件生成


原始信息
明文BIN文件
AES KEY
PUBKEY
PUBKEY_N
AES
RSA
Image文件
Image头
密文BIN文件
KEY的密文
PUBKEY_N

加密固件启动


开始
BOOTROM在跳转二级BOOT之前，获取公钥加密的AES秘钥密文
将获取的密文设置给硬件Flash控制器
硬件Flash控制器使用W800芯片内置的私钥解密得到AES秘钥
硬件Flash控制器在MCU取指令时，用AES秘钥解密后交给MCU执行
跳转到BOOT
Image头
密文BIN文件
KEY的密文
PUBKEY_N

防拷贝

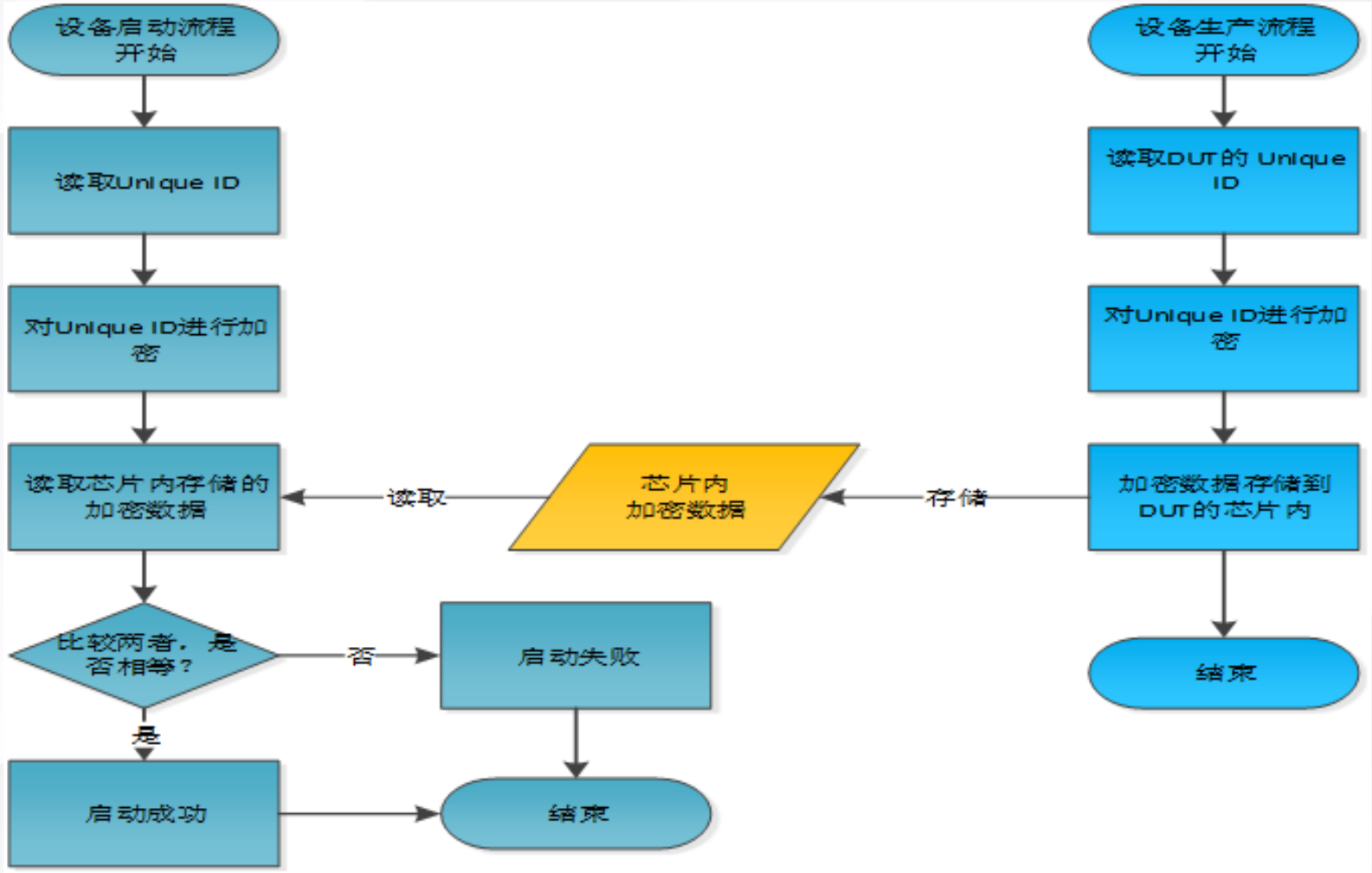
W800拥有唯一的Unique ID（144bit）

W800固件防拷贝流程，分为设备启动流程和设备生产流程.

生产阶段，通过获取Unique ID并对其进行封装处理，写入芯片内部存储器。

启动阶段，通过增加对Unique ID的校验比对流程，保证固件不能被随意拷贝运行。

防拷贝流程


设备启动流程开始
读取Unique ID
对Unique ID进行加密
读取芯片内存储的加密数据
比较两者，是否相等？
否
启动失败
是
启动成功
结束
读取
芯片内加密数据
存储
设备生产流程开始
读取DUT的 Unique ID
对Unique ID进行加密
加密数据存储到DUT的芯片内
结束

联盛德官网：www.winnermicro.com

技术问答社区：
ask.winnermicro.com

微信公众号：
联盛德微电子