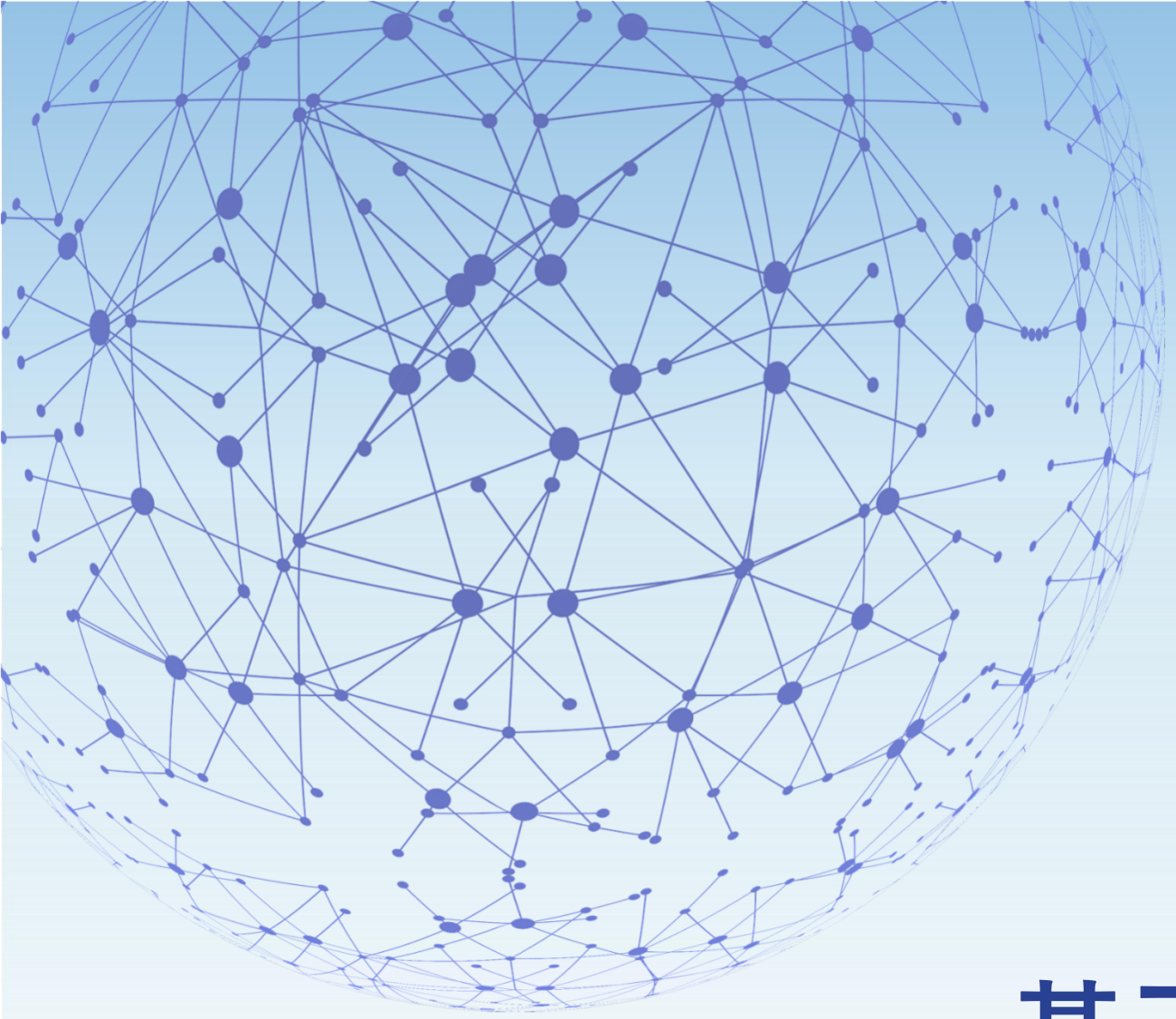


芯来科技
NUCLEI

基于RISC-V的HSM方案

目录

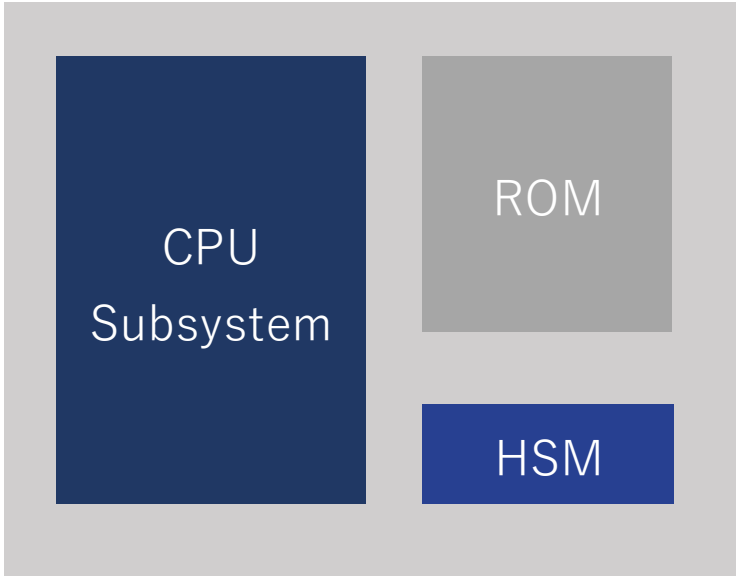
芯来科技
NUCLEI

硬件安全模块HSM —— Hardware Security Module

芯来科技 NUCLEI

HSM 通常用于**金融、医疗保健、政府和云计算**等各个行业，以保护敏感数据和加密密钥免遭未经授权的访问和攻击；在**汽车电子**领域，HSM的使用尤其广泛

HSM在**增强数据安全**和确保敏感信息的**完整性**和**机密性**方面发挥着关键作用



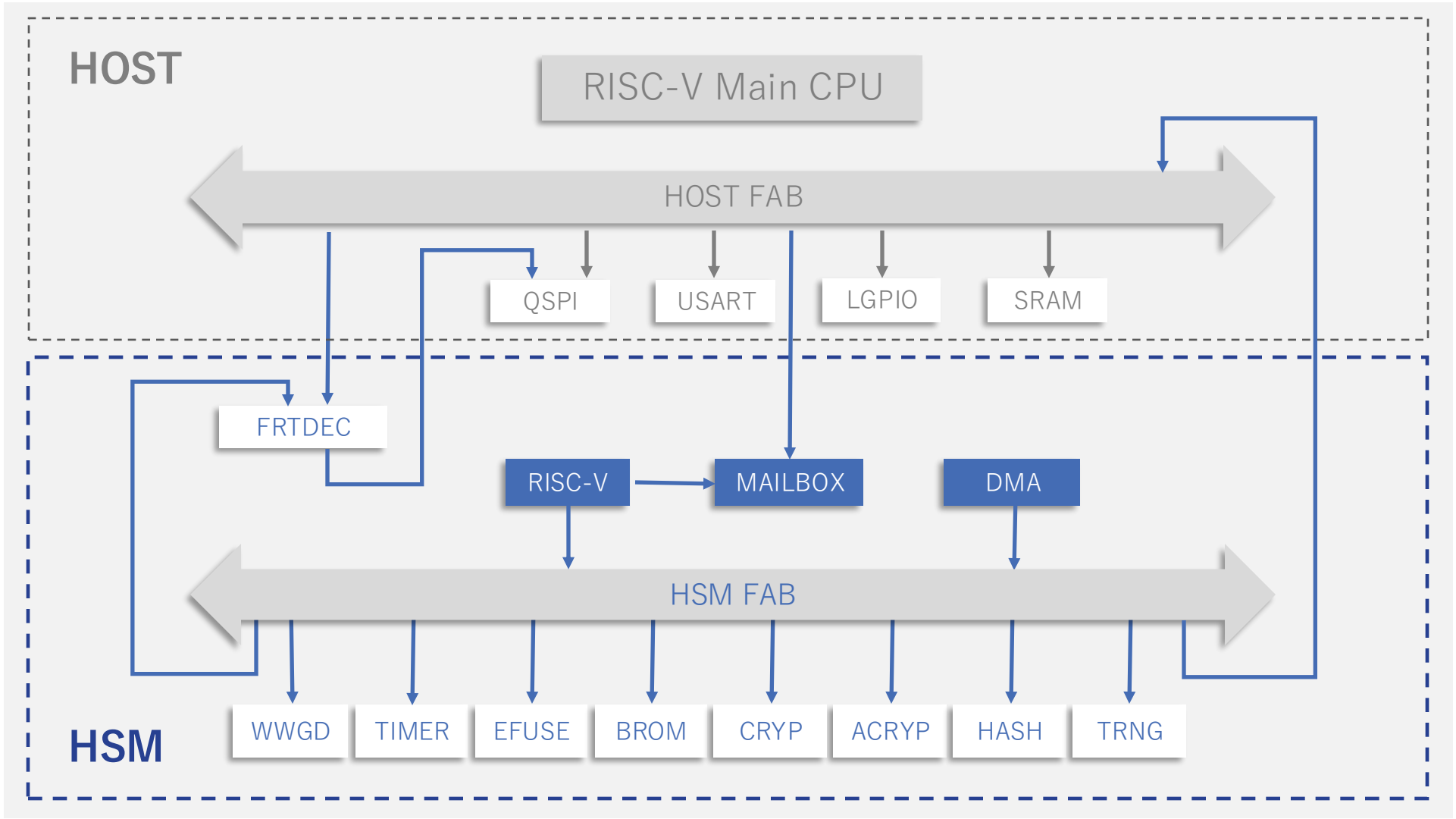
随着芯片集成度的不断提升，HSM已经可以被完整的集成到SoC之中：

- HSM和主CPU子系统紧耦合，安全性更高
- 无需额外引脚与外接安全芯片链接，整体面积更小
- 支持更多丰富的安全启动方案
- 实现可编程安全内核，拥有灵活的扩展性，应用领域更广

芯来科技基于RISC-V的HSM系统架构

芯来科技 NUCLEI

HSM系统架构灵活可配，配合主CPU系统提供更完善的整体解决方案

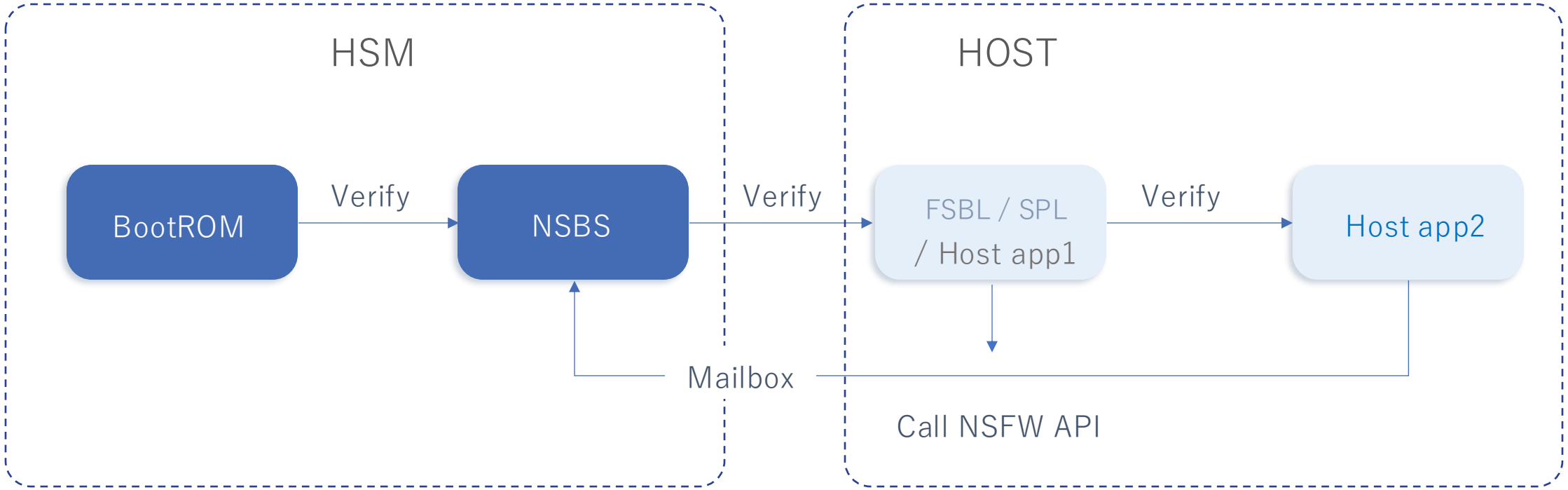


安全启动流程

芯来科技 NUCLEI

典型的HSM安全启动流程：

从HSM BootRom开始进行逐级验证启动，HSM完成HOST端SPL/FSBL代码启动后，将执行NSBS固件代码，等待HOST端通过Mailbox来申请安全服务，支撑HOST端的安全操作

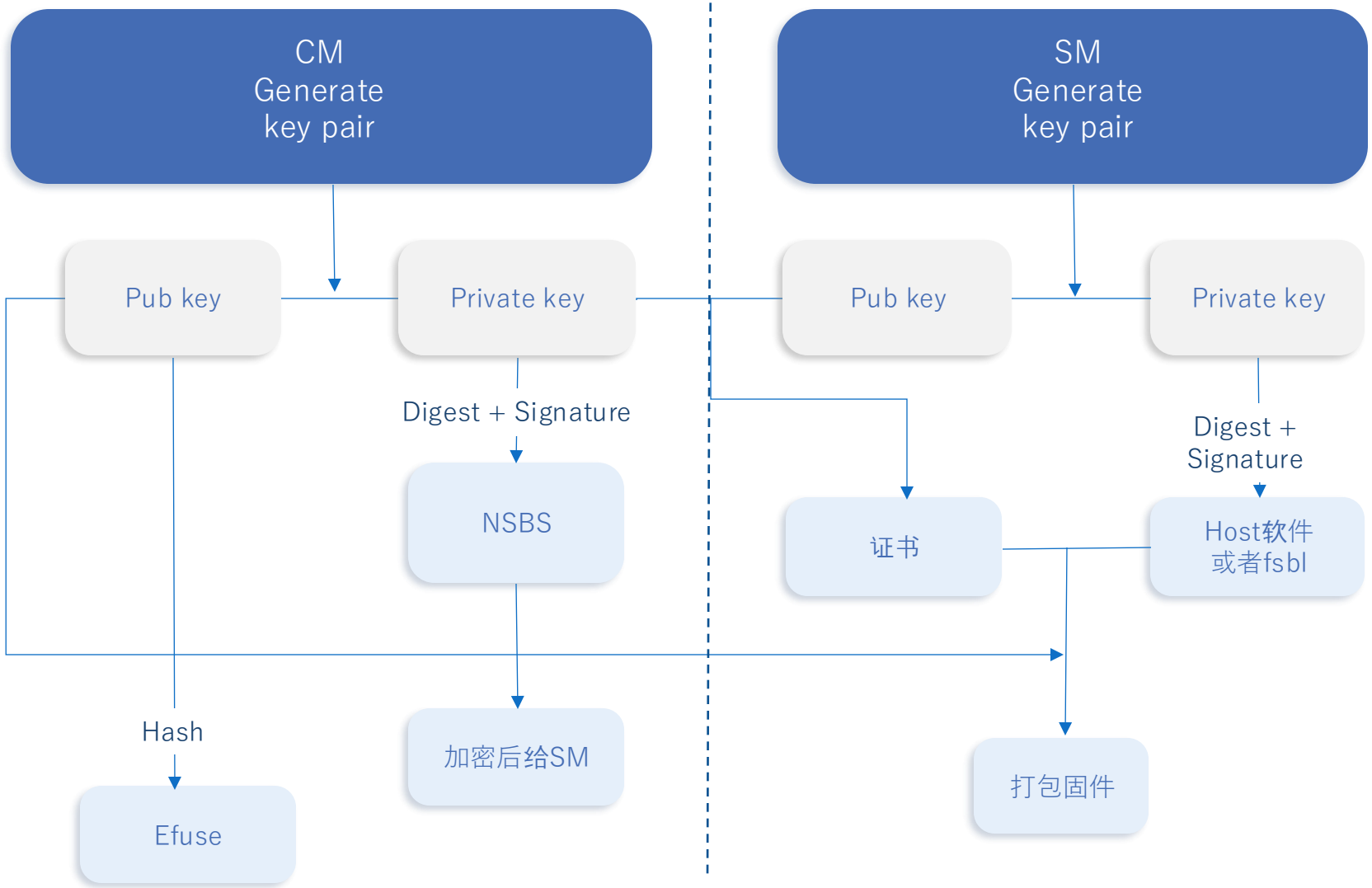


NSBS：Nuclei Secure Boot and Service

非对称认证流程

芯来科技
NUCLEI

- CM和SM各自拥有独立密钥对
- 支持RSA2048，ED25519和SM2验签算法
- 硬件加速器实现验签算法



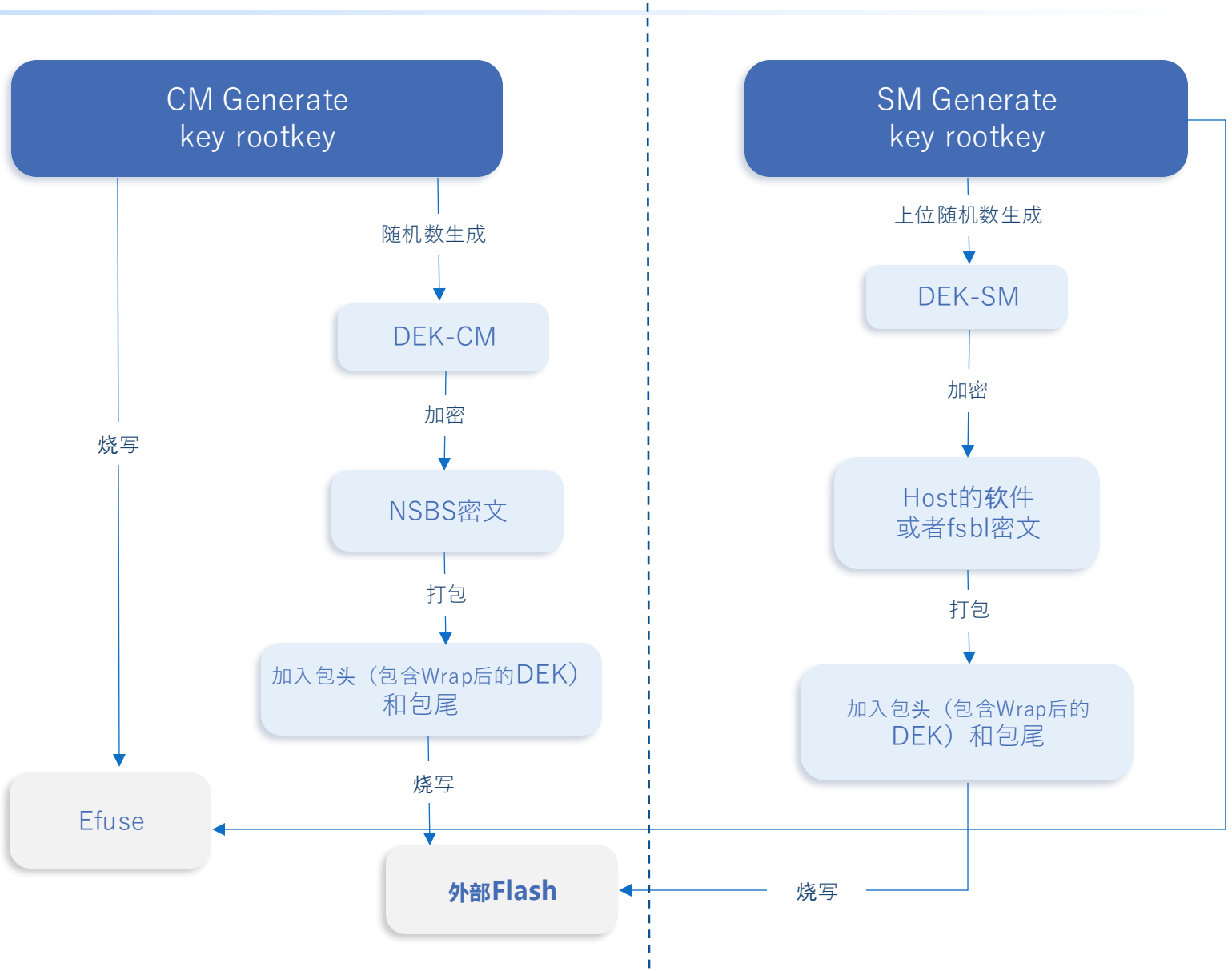
CM：Chip Manufacturer

SM：System Manufacturer

对称加密流程

芯来科技 NUCLEI

- CM和SM各自拥有根密钥
- 支持AES和SM4加解密算法
- 硬件加速器实现加解密算法
  - CM: Chip Manufacturer
  - SM: System Manufacturer
  - FRK: Firmware Root Key
  - DEK: Data Encrypt Key
  - Key Wrap: RFC3394 定义的一种基于AES密钥封装的算法
  - GB/T 36624-2018定义的基于SM4的密钥封装算法



HSM Secure boot Demo方案

芯来科技 NUCLEI

Demo方案支持12种安全启动组合，支持动态选择：

算法组合	验签	解密	摘要
1	RSA2048	AES(128/256)	SHA256
2	RSA2048	\	SHA256
3	RSA4096	AES(128/256)	SHA384
4	RSA4096	\	SHA384
5	ED25519	AES(128/256)	SHA256
6	ED25519	\	SHA256
7	SM2	SM4(128/256)	SM3
8	SM2	\	SM3
9	RSA2048	Frtdec(AES-CTR)	SHA256
10	RSA4096	Frtdec(AES-CTR)	SHA384
11	ED25519	Frtdec(AES-CTR)	SHA256
12	SM2	Frtdec(AES-CTR)	SM3

Demo方案支持全流程系统仿真：

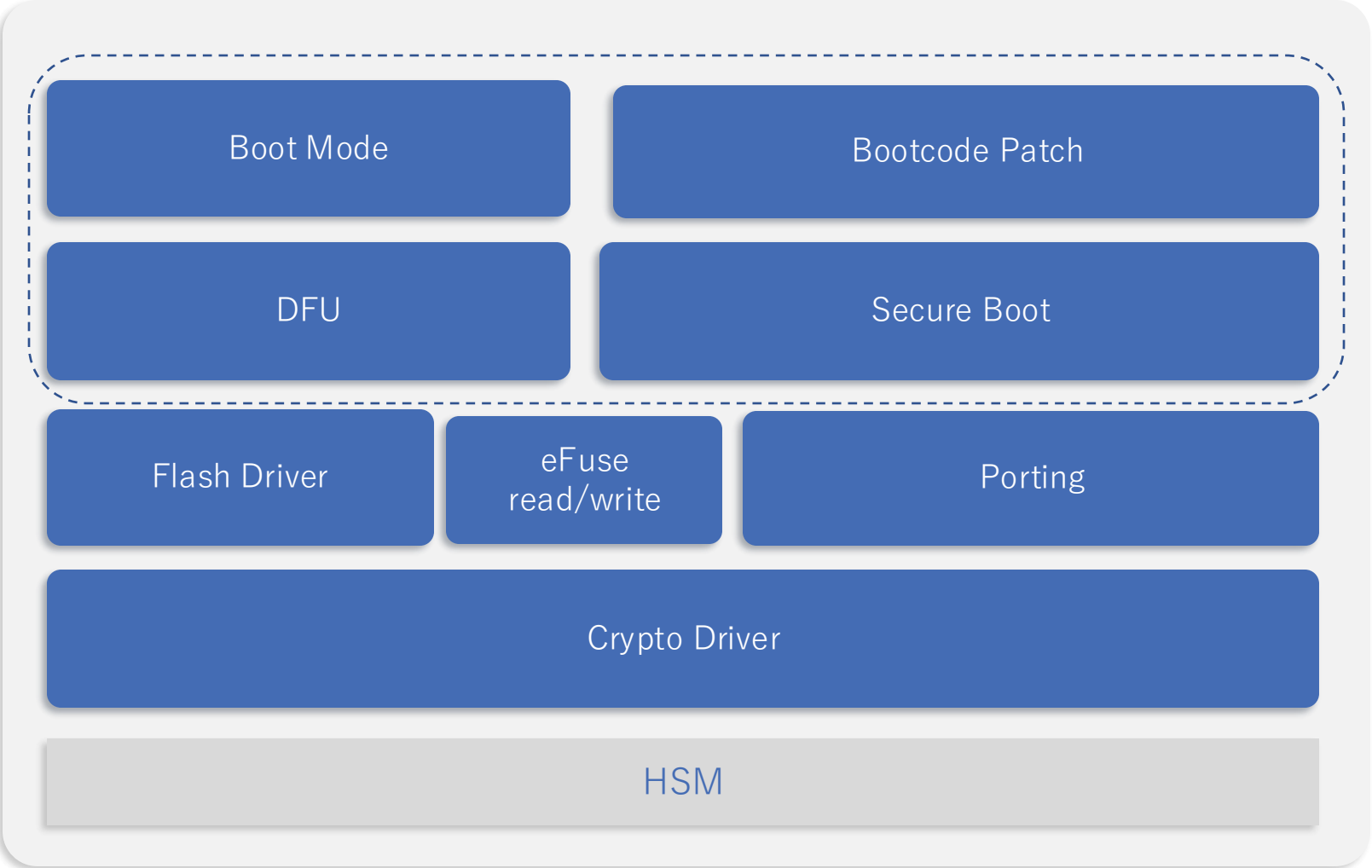
- 提供模版配置文件，一键加密打包脚本以及生成eFuse配置文件
- 支持两级安全启动全流程仿真

Demo方案提供完整的FPGA测试环境：

- FPGA环境下支持仿真环境下相同原始固件
- 提供功能丰富的上位机工具，支持生成并烧写eFuse配置文件和打包原始固件，不需要额外的烧写工具

HSM BootROM

芯来科技 NUCLEI



DFU:

- 自动探测波特率
- UART载程序到SRAM中执行
- UART烧写程序到Flash中执行

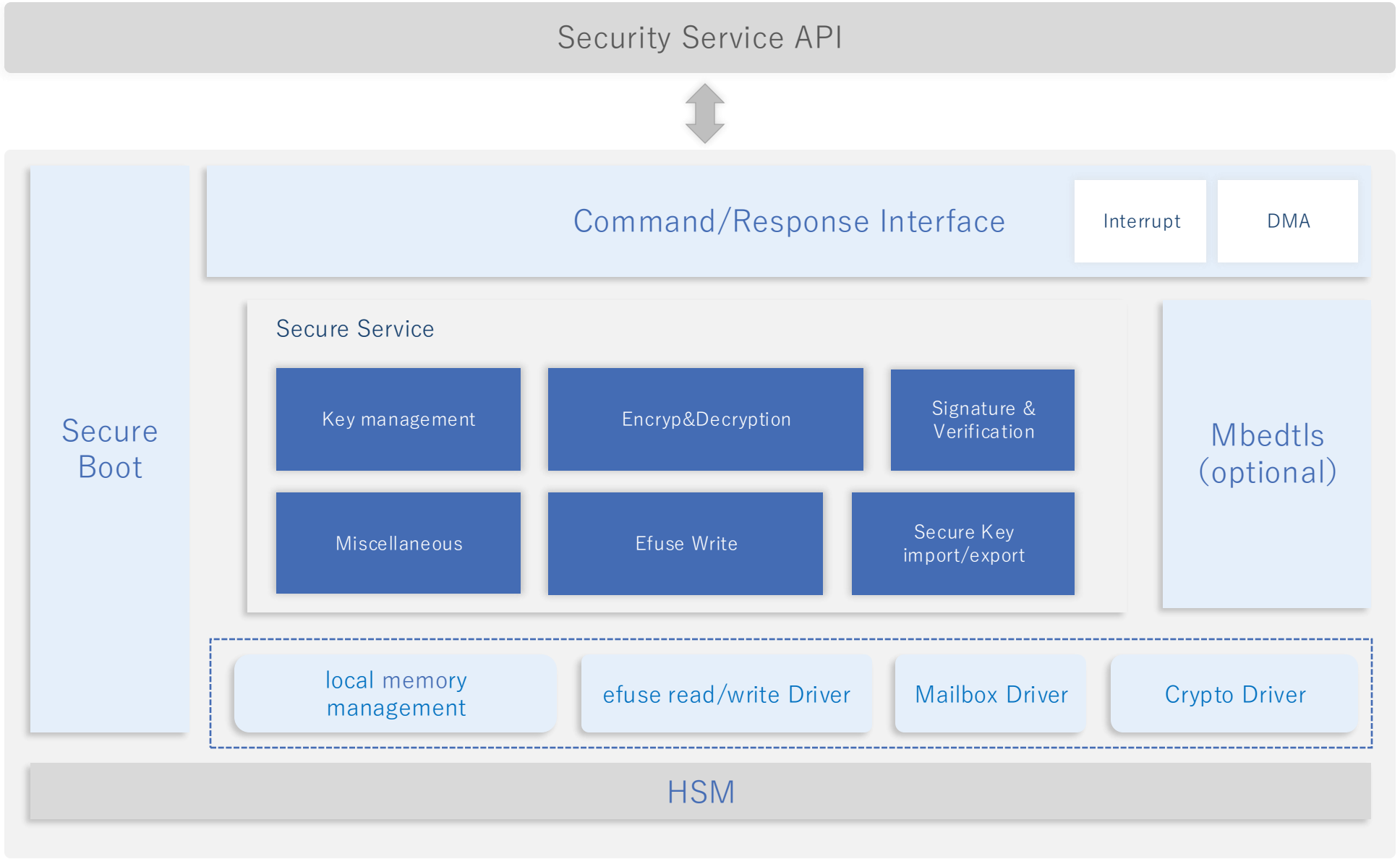
Boot Mode:

- 支持多种启动模式

Bootcode Patch：

- 支持bootcode修补

Nuclei Secure Boot and Service (NSBS)



eFuse/flash内容格式

芯来科技 NUCLEI

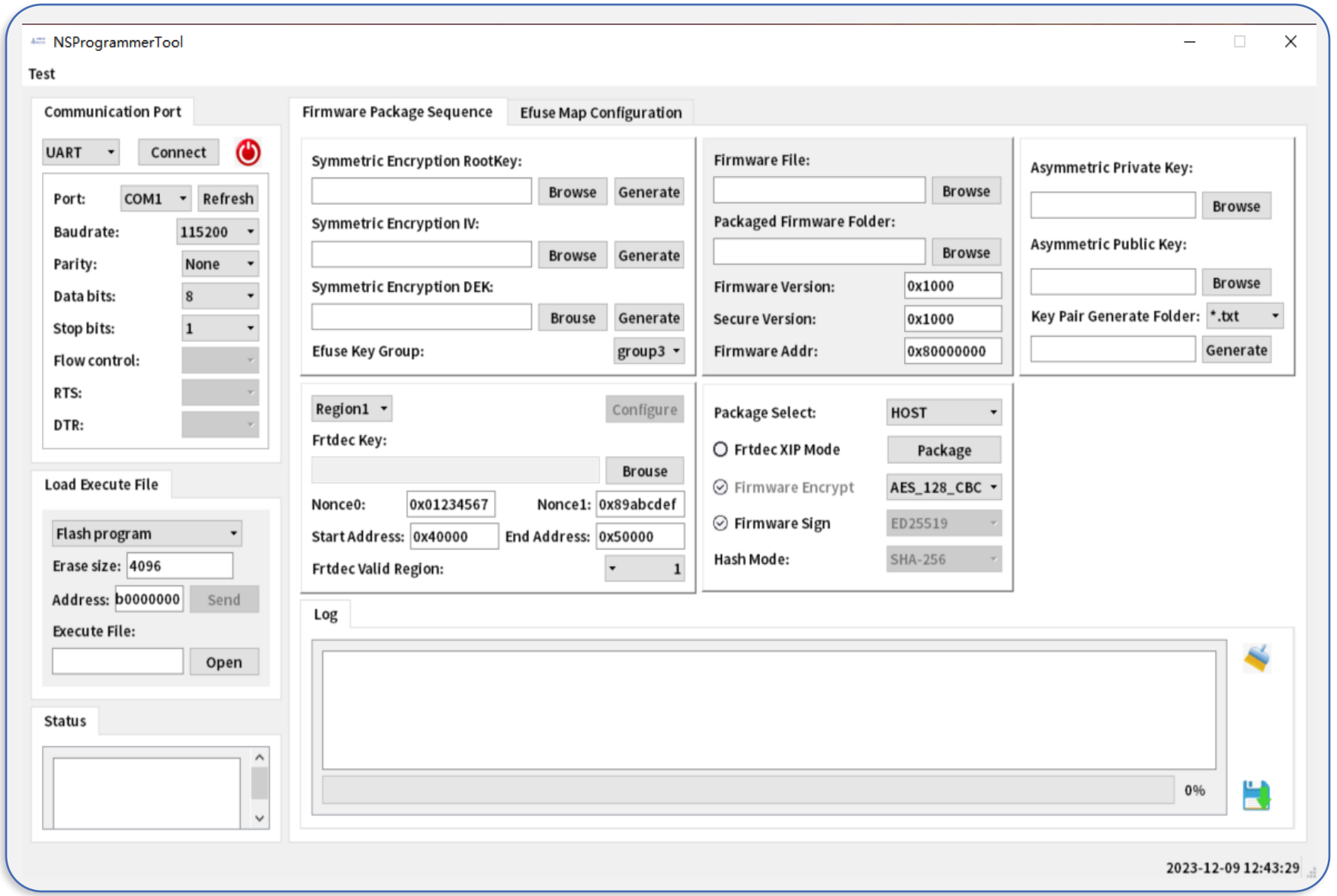
eFuse 映射表

Boot Configuration
Secure Boot Configuration
CM Public Key Digest
SM Public Key Digest
CM Public key Monotonic Counter
SM Public key Monotonic Counter
CM Rootkey
SM Rootkey
Version Monotonic Counter
Life Cycle

固件 结构表

Boot Configuration
Payload
Payload Digest
Payload Digest Signature
DEK（wrapped）
Public Key

上位机工具NSTools



固件打包功能：

- 支持两级镜像的打包，多级密钥生成
- 根据UI界面的配置，生成固件头，加密固件，计算固件摘要和签名，生成打包后bin文件；
- 根据配置生成eFuse配置文件

烧写功能：

- DFU：烧写或者擦除指定的扇区，页和整片；
- eFuse烧写：单bit或者单word烧写;根据生成或者指定的eFuse配置文件进行批量烧写；

芯来科技HSM的其他增强安全特性

芯来科技
NUCLEI

安全存储

- 支持flash数据通路上的on-the-fly解密

锁定软件bootloader更新

- 支持限制软件bootloader，提高安全性

密钥销毁

- 支持备份密钥
- 支持密钥销毁

生命周期管理

- 开发模式
- 量产模式

防止代码回滚

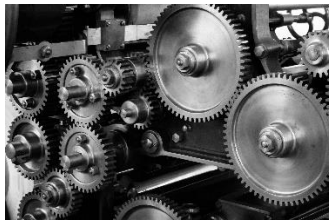
- 支持固件版本管理

支持备份镜像，支持多种加解密算法

芯来科技HSM已经实现落地并被广泛的使用在各类领域

芯来科技 NUCLEI

HSM



工业控制

汽车电子

通讯

网络

芯来科技
NUCLEI

芯来科技公众号

THANK YOU