海思网络安全白皮书

文档版本　02

发布日期　2023-11-16

注意

您购买的产品、服务或特性等应受海思公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，海思公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

海思技术有限公司

地址：　　上海市青浦区虹桥港路 2 号 101 室　　邮编：201721

网址：　　http://www.hisilicon.com

客户服务邮箱：　　support@hisilicon.com

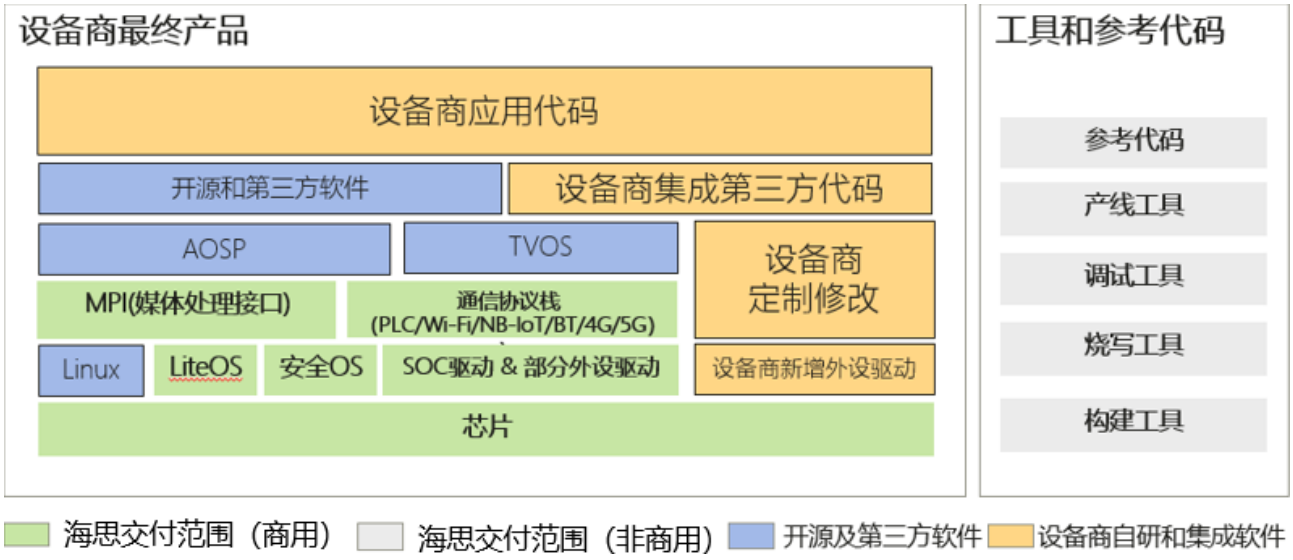
目 录

1 概述

海思技术有限公司（以下简称“海思”）是全球领先的 Fabless 半导体设计公司，面向城市、家庭及出行三大应用场景，提供领先、创新、安全可靠的芯片与解决方案，覆盖智慧视觉（Camera）、智慧媒体（STB/TV 等）、AIOT(人工智能物联网)及智慧出行等多个领域；

海思业务是面向开发者的业务，向设备商交付芯片、SDK（LiteOS、安全 OS、SOC 驱动&部分外设驱动、UNF/MPI（媒体处理接口）、通信协议栈（PLC/Wi-Fi/NB-IOT/BT/4G/5G）、工具、参考代码、开源及第三方软件、资料等）。设备商基于海思的交付包，定义、设计、开发、测试、发布、生产、维护自己的产品。图 1-1 给出了海思的业务交付界面。

图1-1 业务交付界面



业务交付界面

1. 海思交付范围（商用）：芯片、SDK（LiteOS、安全 OS、SOC 驱动&部分外设驱动、UNF/MPI（媒体处理接口）、通信协议栈（PLC/Wi-Fi/NB-IOT/BT/4G/5G）、开源及第三方软件、资料等）。
2. 海思交付范围（非商用）：工具和参考代码。
3. 设备商交付范围：设备商除了负责开发应用层代码，还会根据其产品需求，对海思交付的代码进行新增、修改和删除。

网络安全责任模型

海思不直接向最终用户销售芯片产品，海思向设备商销售芯片、SDK 和资料；设备商根据自身产品需求，对海思交付代码进行新增、修改和删除，因此我们无法对最终用户的终端产品提供技术支持；如果您在使用含有海思芯片产品时遇到问题，请与设备提供商联系以寻求直接的技术支持。

基于图 1-1 业务交付界面，网络安全责任模型如下。

1. 海思对交付的芯片、SDK（LiteOS、安全 OS、SOC 驱动&部分外设驱动、UNF/MPI(媒体处理接口)、通信协议栈（PLC/Wi-Fi/NB-IOT/BT/4G/5G）、资料等）提供基础的网络安全技术，对包含在 SDK 中的开源及第三方软件提供漏洞修补方案；并根据合同约定提供网络安全支持。
2. 海思交付的 SDK 中工具仅供设备商开发调试使用、参考代码仅供设备商演示芯片功能使用，不属于商用交付范围，海思不对该部分代码作出任何形式的保证和承诺。
3. 设备商除了负责开发应用层代码，根据其产品需求，基于海思提供的 SDK，可以在任一层新增、修改代码，设备商对自己新增加的代码和针对海思交付范围进行修改的代码负网络安全责任。

作为一家全球领先的 Fabless 半导体设计公司，海思致力于与各利益相关方密切合作、持续创新、共建标准，确保我们提供的芯片和解决方案的完整性和安全性能够满足或超越我们设备商的需求，并为他们的客户提供必要的保障信心。

2 基础技术安全

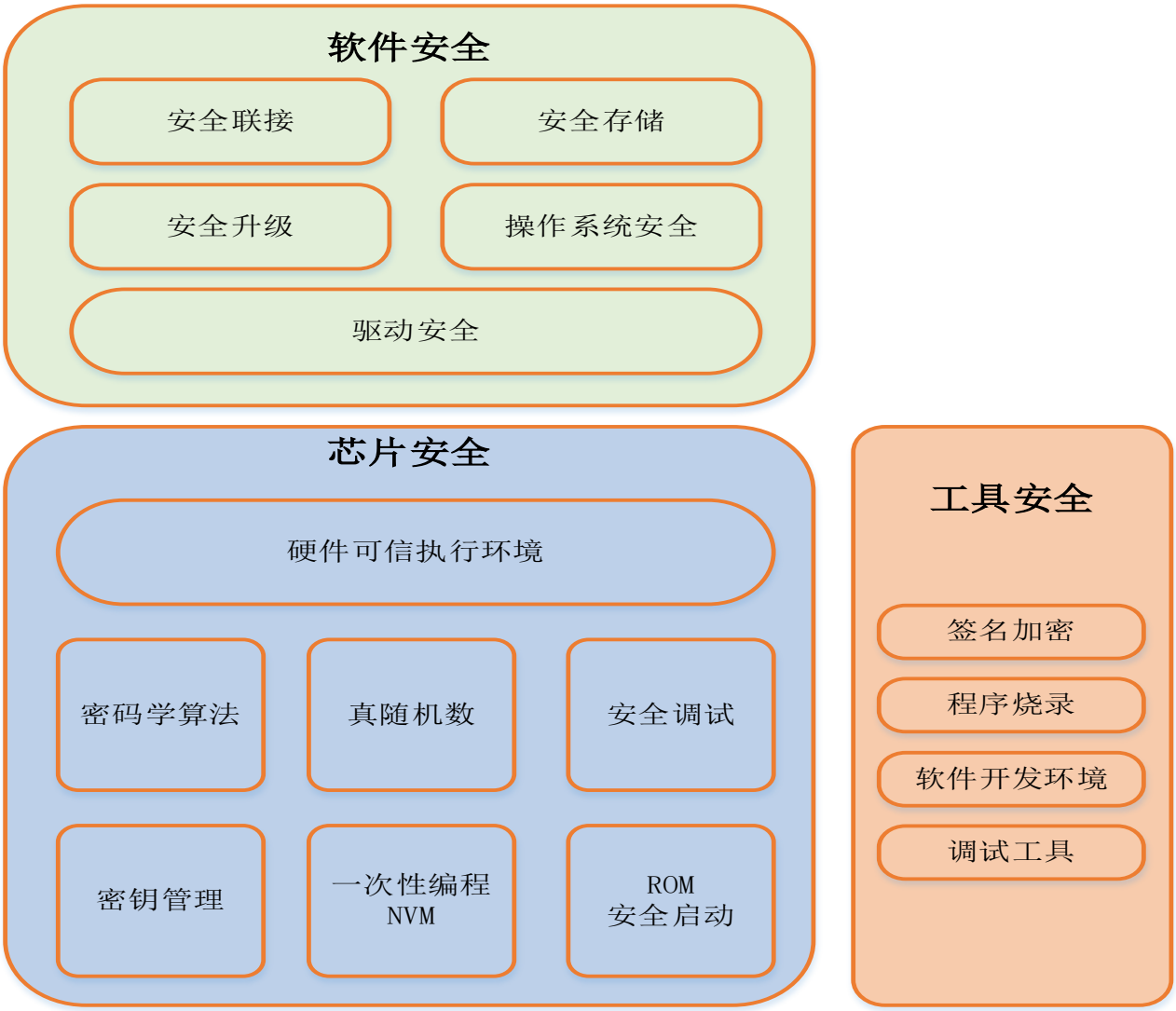
安全系统通常建立在硬件安全的基础之上，为关键服务和应用程序的运行提供安全基础平台，海思在芯片中提供了一系列的硬件基础安全技术供设备商选择使用，帮助设备商打造安全可信的终端设备。本章节主要描述海思在硬件芯片上的基础安全技术。

2.1 基础技术安全架构

海思提供芯片、软件和工具一系列的安全技术，帮助设备商快速构建安全可信的产品与解决方案。

- 硬件安全：芯片安全启动、安全调试、一次性可编程 NVM 用于存储密钥与 ID、密钥管理、密码学算法等提供了硬件级的安全基石。硬件可信执行环境为安全软件的运行和构建安全的解决方案提供了保障。
- 软件安全：操作系统和驱动安全，以及关键服务如安全存储、安全联接、安全升级等，为网络安全构筑了基本屏障，是设备商进一步开发完整安全产品的基础组件。
- 工具安全：签名加密、程序烧录、软件开发环境、调试工具等，使设备商基于海思的芯片平台可以高效快速的开发出有竞争力的安全产品和解决方案。

图2-1 安全技术总体架构

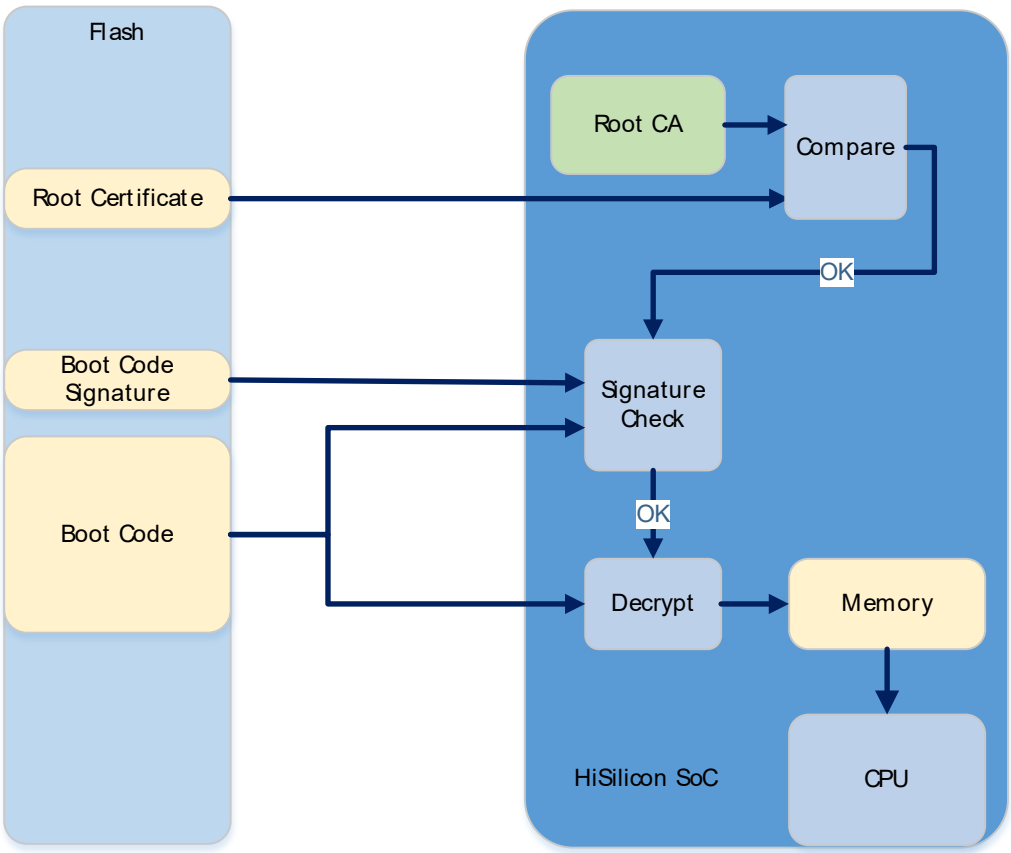


2.2 安全启动

芯片从片上 BootROM 启动，为系统提供根信任。这个不可变的 BootROM 代码是原生可信的也是软件信任链的起点。BootROM 代码执行的第一个任务是验证外部根公钥是否与芯片内一次性可编程器件存储的根公钥一致，然后使用该可信的根公钥来验证外部一级启动代码和其对应的参数配置签名是否正确，只有通过验证的外部一级启动代码才会被执行。一级启动代码也支持加密，其加密密钥也来自芯片内一次性可编程器件存储的根密钥派生。经过验证的外部可信一级启动代码，进而可以采用类似机制进一步验证其他软件代码，形成整个信任链。

除 Flash 外，芯片也可以支持其他启动媒介，例如串口设备、SDIO 设备、USB 设备等。在这种情况下，BootROM 从启动媒介获取根公钥和引导代码，并采用相同的方式进行启动验证，整个启动引导过程都使用国际认可的标准算法和协议。

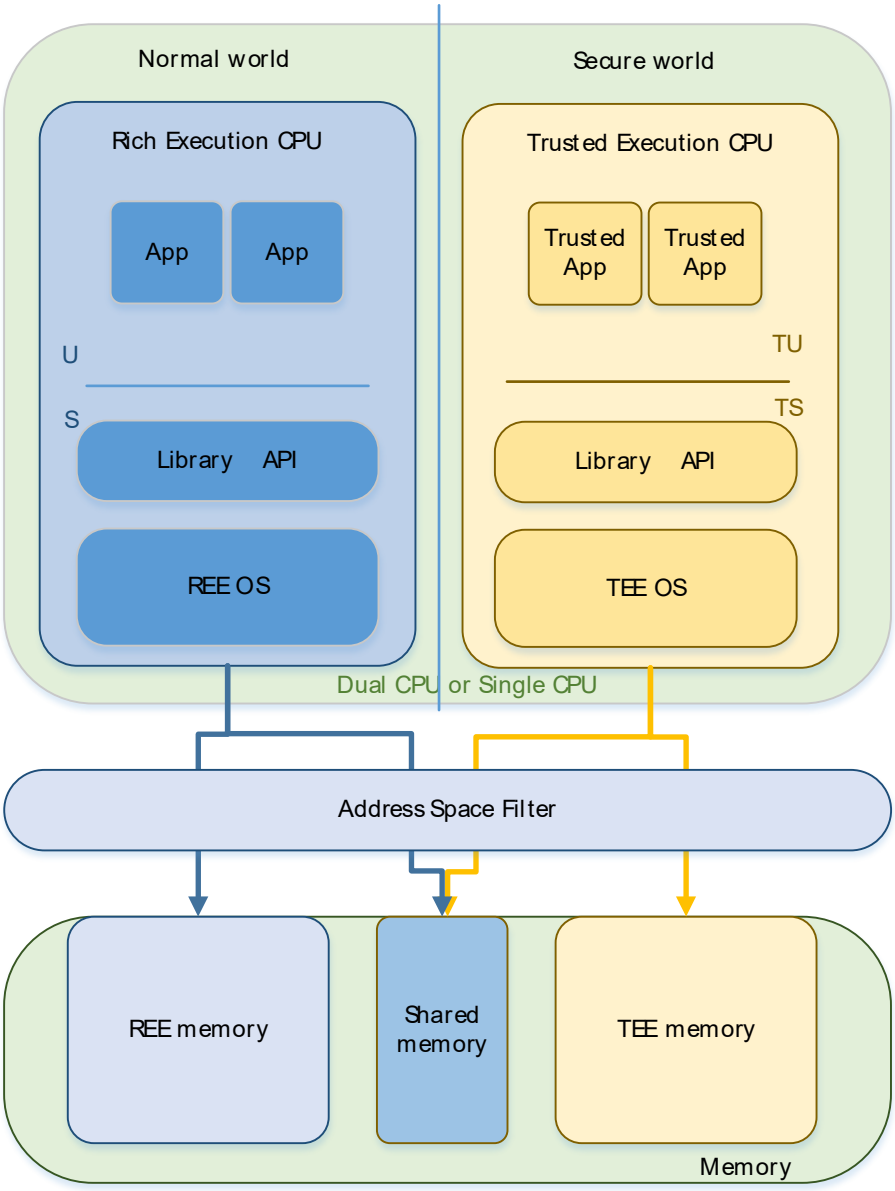
图2-2 安全启动



2.3 可信执行环境

为实现关键业务计算和敏感数据的安全访问，芯片支持将系统划分为安全世界（Trusted Execution Environment，TEE，也叫可信执行环境）和非安全世界（Rich Execution Environment，REE，也叫普通执行环境）。根据不同芯片的特点，可以是将一个独立完整的 CPU 工作状态指定在安全世界，也可以通过使用分时复用处理器来实现；例如 ARM TrustZone 技术。安全世界和非安全世界对内存的访问是分区隔离的，每个世界只能访问指定给它的内存。安全世界和非安全世界也分别有各自的加解密硬件资源和外设资源。iTrustee 安全 OS 为关键业务计算和敏感数据的安全访问提供了一个可信执行环境。

图2-3 可信执行环境



iTrustee 安全 OS 介绍

iTrustee 安全 OS 是华为基于 ARM TrustZone 技术实现的可信执行环境，TrustZone 是硬件级别的安全，它将处理器的工作状态划分为 TEE 和 REE，分别执行 TEE OS 和 REE OS，通过特殊指令在处理器的 TEE 和 REE 之间切换来提供硬件隔离。在 TEE 下，提供了对硬件资源的保护和隔离，包括内存、外设等，通过执行过程保护、密钥保密性、数据完整性和访问权限控制实现了端到端的安全，可防止来自 REE 的恶意软件攻击。iTrustee 安全 OS 提供的基础安全能力有：

可信存储服务

提供关键信息的存储能力，保证数据的机密性、完整性。可信存储支持设备绑定，支持不同安全应用之间的隔离，每个安全应用仅能访问自己的存储内容，无法打开、删除或者篡改其他安全应用存储的内容。iTrustee 安全 OS 的可信存储分为两种：安全文件系统存储和 RPMB（Replay Protected Memory Block）存储，前者将密文存储到特定的安全存储分区，后者存储到 eMMC 器件特定的存储分区，RPMB 存储还支持防删除、防回滚特性。

加解密服务

iTrustee 安全 OS 支持多种对称、非对称加解密算法以及密钥派生算法，支持同一芯片平台相同密钥的派生，支持设备唯一密钥，支持国际标准加密算法，支持国密算法，遵从 Global Platform TEE 标准，为第三方开发存储和使用密钥的业务 TA（Trusted Application，可信应用）提供支持。为提高安全性，iTrustee 安全 OS 内部的密钥生成和计算，采用的是独立的安全硬件和经过安全加固的软件完成，整体方案经过了国际安全认证实验室的认证。派生的密钥将被存储在独立的安全存储芯片中，或者经过严格加密的安全存储空间中。用户可以根据业务的需要，开发 TA 来使用可信密钥服务。

可信时间

iTrustee 提供可信的基准时间，该时间不能被恶意 TA 或者 REE 修改。

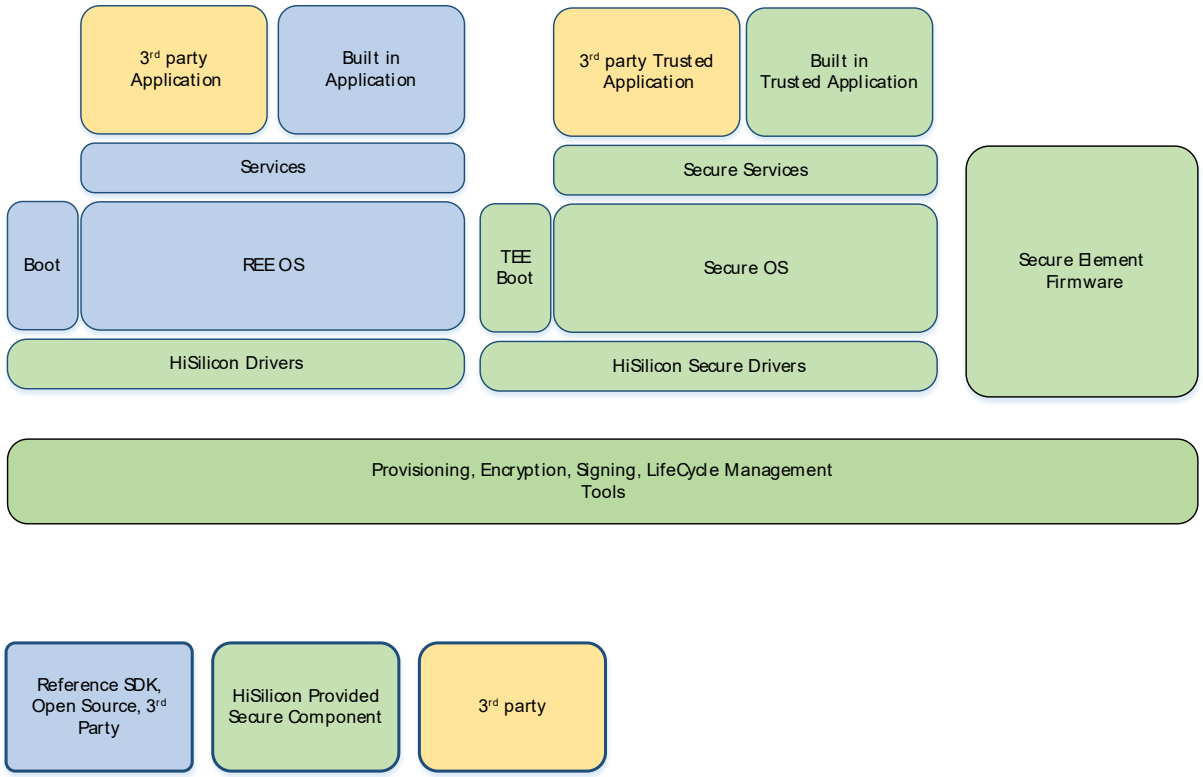
2.4 安全软件组件

为了使系统从可信执行环境中获益，必须对在这个隔离的安全世界中运行的软件也进行加固，以防止逻辑攻击和物理攻击。这可以为设备的密钥和数据提供更高的安全保证。海思提供关键安全软件组件，预集成到芯片和 TEE 中，方便快速、简单地开发出安全健壮设备。

安全操作系统与所需的安全服务（如加密、安全存储）一起提供。这些安全操作系统可以运行来自 OEM 或第三方的受信任应用程序，或者仅将内置的受信任应用程序用于常用的安全功能。安全操作系统、受信任的应用程序、底层硬件驱动程序和安全引导程序都经过内部和外部专家的仔细审查，以确保抵御攻击的健壮性。包含嵌入式安全单元的芯片所需的固件也根据需要支持外部机构安全认证。

在安全系统允许这些软件组件执行之前，这些组件需要经过加密和数字签名，海思提供了相应的工具来简化这一过程，并确保只能执行经过验证的代码。

图2-4 安全软件组件



2.5 一次性可编程器件

每台设备的唯一身份是物联网安全的关键要求之一，以便对物联网系统内的设备进行安全认证和授权。唯一的对称密钥也为更一般的安全存储加密提供了基础。用于软件验证的非对称密钥也必须永久绑定到设备。这些关键信息都通过芯片内置的一次性编程器件存储。

2.6 硬件密钥管理

对称密钥只能由芯片内的密钥派生硬件模块用密码学算法派生（支持 AES 或 PBKDF2），由此产生的密钥只能由芯片内加解密硬件使用，用于加密或解密数据。芯片内的根密钥以及派生密钥对软件不可访问。

2.7 密码学算法

海思芯片支持多种国际标准的密码学算法和密钥模式，并提供防侧信道攻击能力，包括常用对称算法 AES/TDES 和公钥算法 RSA/ECC 等。部分芯片支持国密算法。

2.8 真随机数

密码学和安全协议中通常使用随机数来防止重放攻击和中间人攻击。为了确保维护安全所必需的随机数的质量，芯片提供一个基于硬件的真随机数发生器。CPU 可以读取并利用这些随机数来建立安全通信或其它密钥派生的基础。

2.9 调试保护

JTAG 调试和测试端口可以通过芯片硬件密码锁定，以防止数据和代码被非法提取，或通过调试端口劫持正在运行的系统。每颗芯片都采用唯一的密码进行锁定，海思提供工具读取设备标识并提供解锁调试端口所需的密码。芯片也支持调试端口通过一次性编程永久关闭。

3 工程安全

海思适配并发布了一套适合芯片业务开发场景的网络安全开发流程，本章除了对流程的介绍，还会重点描述安全设计、安全编码、安全测试、第三方软件管理等安全工程能力的具体实践。

3.1 网络安全流程

海思适配并发布了一套适合芯片业务开发场景的网络安全开发流程，将安全活动融入产品的研发活动中，如图 3-1 所示。

图3-1 网络安全流程

3.2 安全需求和设计

海思遵从法律法规、行业标准，参考业界安全设计原则和公司制定的安全规范，在安全需求和设计阶段根据业务场景、展开安全威胁分析。威胁分析使用业界通用的 STRIDE 威胁建模方法。当识别出威胁后，设计工程师会根据公司积累的安全削减库、安全设计方案库制定威胁消减措施，并完成对应的安全方案设计。所有的威胁消减措

施最终都将转换为安全需求、落入开发流程，同时后端测试工程师会针对安全需求设计测试用例完成安全需求的测试验证，最终保障交付产品的网络安全。

3.3 安全编码

海思严格遵从公司对内发布的安全编码规范，安全研发和测试人员在上岗前均通过了对应规范的学习和考试。同时引入了业界领先的静态代码扫描工具进行每日检查，其结果数据进入持续集成和持续部署工具链，通过代码质量门限进行控制，以评估产品代码的安全质量。所有产品项目在发布前，均需完成静态代码扫描的告警清零，有效降低产品编码相关的安全问题。

3.4 安全测试

海思所有项目发布前都经过了多轮安全测试，包括但不限于开发阶段的高风险接口的白盒测试，测试阶段通过对软件外部接口和协议的 fuzzing 灰白盒测试，公司内部安全测试专家安全专项测试。测试用例覆盖安全设计阶段识别出的安全需求以及攻击者视角的渗透测试用例。同时将深入理解的客户安全需求和业界标准作为检查项，开发配套相应的安全测试工具。

3.5 安全交付与维护

海思将“二次开发网络安全注意事项”文档随 SDK 提供给设备商，文档中列出了基于海思 SDK 做二次开发时的典型安全注意事项（如产品化后如何关闭调试端口等）。

海思 PSIRT（Product Security Incident Response Team）团队负责接收、调查和披露海思产品和解决方案相关的安全漏洞，是公司对漏洞信息进行披露的重要窗口。海思鼓励漏洞研究人员、行业组织、政府机构和供应商主动将与海思产品相关的安全漏洞报告给海思 PSIRT。上报方式请访问：http://dggsc37-wb.huawei.com/?sc_itemid=%7BC25D4C28-0561-4CBF-9D6E-09CDCDFEFACF%7D&sc_mode=preview&sc_lang=zh。

4 安全认证

本章节主要阐述硬件与芯片、SDK 平台软件遵从的各种安全标准和已经获得的安全认证

安全标准遵从

- GM/T 0002-2012 SM4 分组密码算法
- GM/T 0003-2012 SM2 椭圆曲线公钥密码算法标准
- GM/T 0004-2012 SM3 密码杂凑算法
- GM/T 0008-2013 安全芯片密码检测准则
- GB/T 18336-2015 信息技术 安全技术 信息技术安全评估准则
- ISO/IEC 15408:2009 Information technology-Security techniques — Evaluation criteria for IT security

安全认证

- 内容安全 CAS 领域: Irdeto、Nagra、Viaccess、DCAS、Novel、Suma 安全认证
- 内容安全 DRM 领域：Riscure、ChinaDRMLab、Netflix 等安全认证
- Riscure RAPC 金牌认证
- TÜViT nuSIM 安全认证
- iTrustee 5.0 可信执行环境 CC EAL2+
- 微内核 CC EAL 5+
- 中国信息安全测评中心 EAL3
- 国密安全芯片认证

5 结论

海思非常重视用户的设备安全，提供底层芯片、驱动、安全 OS 等设备的基础安全技术，帮助设备商开发安全可靠的设备产品；在提供基础安全技术的同时，海思非常重视安全流程和安全能力的建设，以实现对产品生命周期的安全管理。海思设立了专门的 CERT 组织，致力于提升产品的安全性。任何发现海思产品安全漏洞的组织或个人，上报方式请访问：http://dggsc37-wb.huawei.com/?sc_itemid=%7BC25D4C28-0561-4CBF-9D6E-09CDCDFEFACF%7D&sc_mode=preview&sc_lang=zh。海思应急响应的同事会在最短的时间内与您取得联系，同时组织内部漏洞的修复，并进行发布漏洞预警和推送补丁更新，海思真诚与您共同构筑设备的安全。

