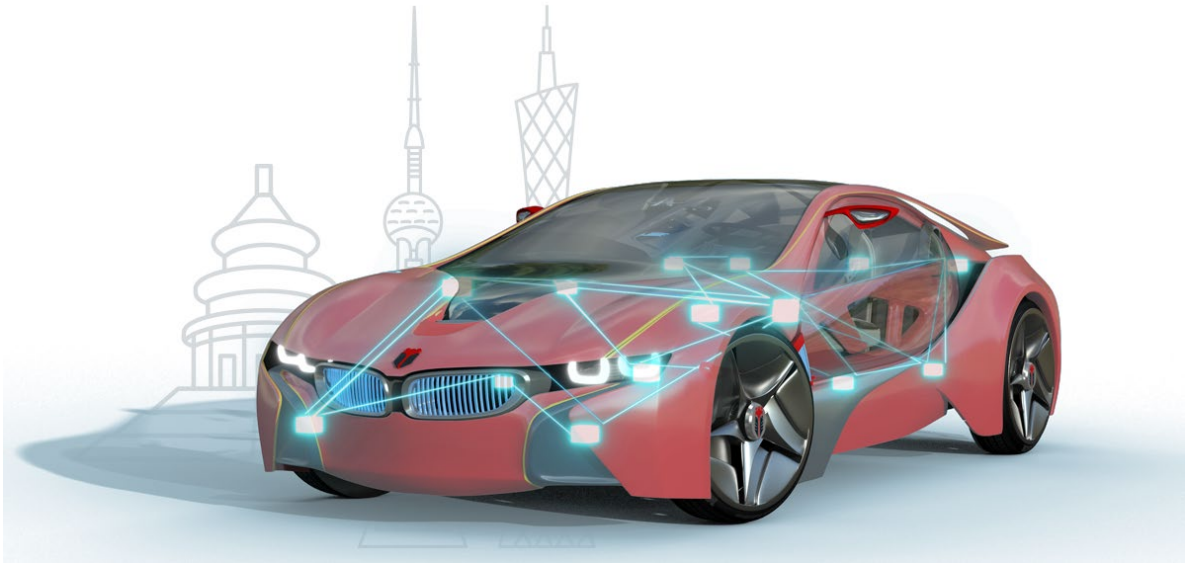
知从木牛信息安全

方案手册

知从®木牛基础软件平台



知从木牛信息安全方案手册

1 方案介绍

知从®木牛基础软件平台

早期的汽车电子是一个比较封闭的系统，不与外界互联，然而随着汽车电子智能化和网联化的发展，信息安全正在占据重要的位置。信息安全 ISO21434 标准也随之出台，汽车电子对信息安全的要求也越来越严格，相关的需求日益增多。

MCU 端的信息安全正式汽车电子信息安全环节中的重要一环，

- 安全启动（SecureBoot）可以有效防止攻击者恶意修改软件；
- 安全诊断（SecureDiagnostic）确保了应用数据不会被第三方获取，避免信息泄露；
- 安全升级（SecureUpdate）保证授权软件才可被控制器使用，搭配安全启动功能有效避免非官方程序被控制器执行
- 安全通信（SecOC）有效确保了整车通信数据安全，防止行车过程中数据被攻击篡改导致危险事故
- 安全调试（SecureDebug）防止控制器内部安全数据被非法导出修改
- 安全存储（SecureStorage）避免控制器数据内部数据被非法软件获取
- 安全日志（SecureLog）可以有效地保护控制器在客户端的信息安全,有效防止控制器被异常篡改和信息窃取,增加整车的安全性,加速汽车电子网联化进程。

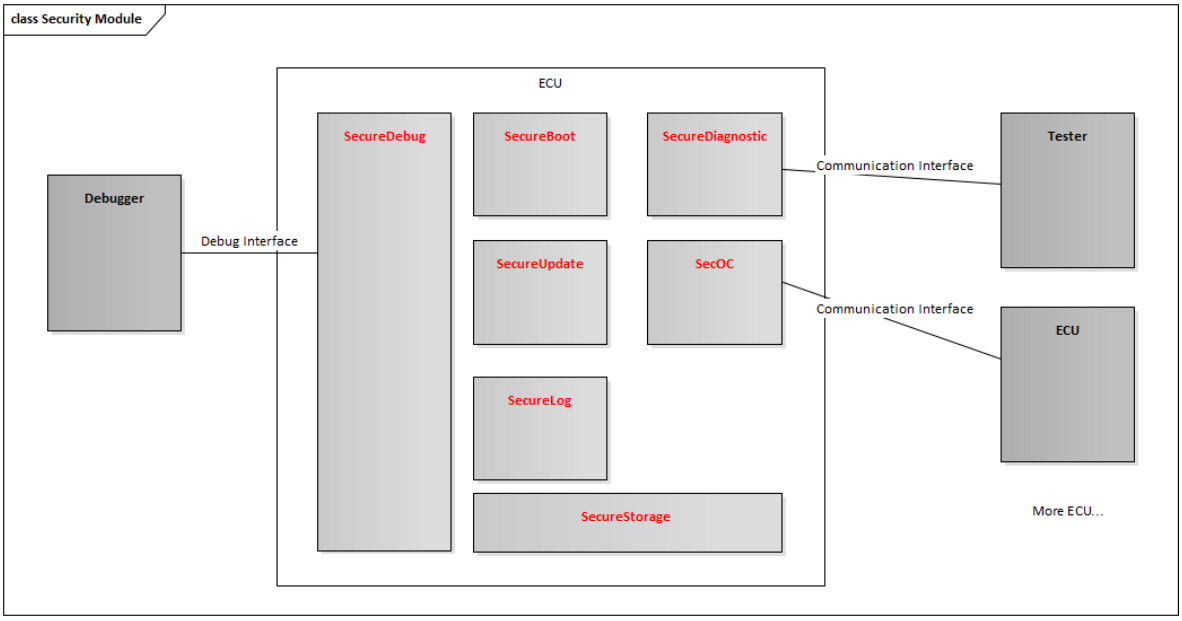


图 1 ECU Security Module

2 安全启动 SECUREBOOT

知从科技可以为客户提供 SecureBoot 完整方案，并可针对项目特定需求和硬件模块定制开发：

- 基于硬件加密方案
- 基于软件加密方案
- 密钥存储管理方案
- 安全启动失效分析
- 产线生产模式方案

安全启动（SecureBoot）是 MCU 的基本功能，通过硬件加密模块来实现，该机制必须独立于用户程序运行，不能被破坏。作为整个安全启动信任链的基础，安全启动主要用于在 MCU 启动之后，用户程序执行之前，对用户定义的 Flash 中关键程序的数据完整性和真实性进行验证，确定是否被篡改。如果验证失败，说明 MCU 处于不可信的状态，部分功能甚至整个程序不能运行。

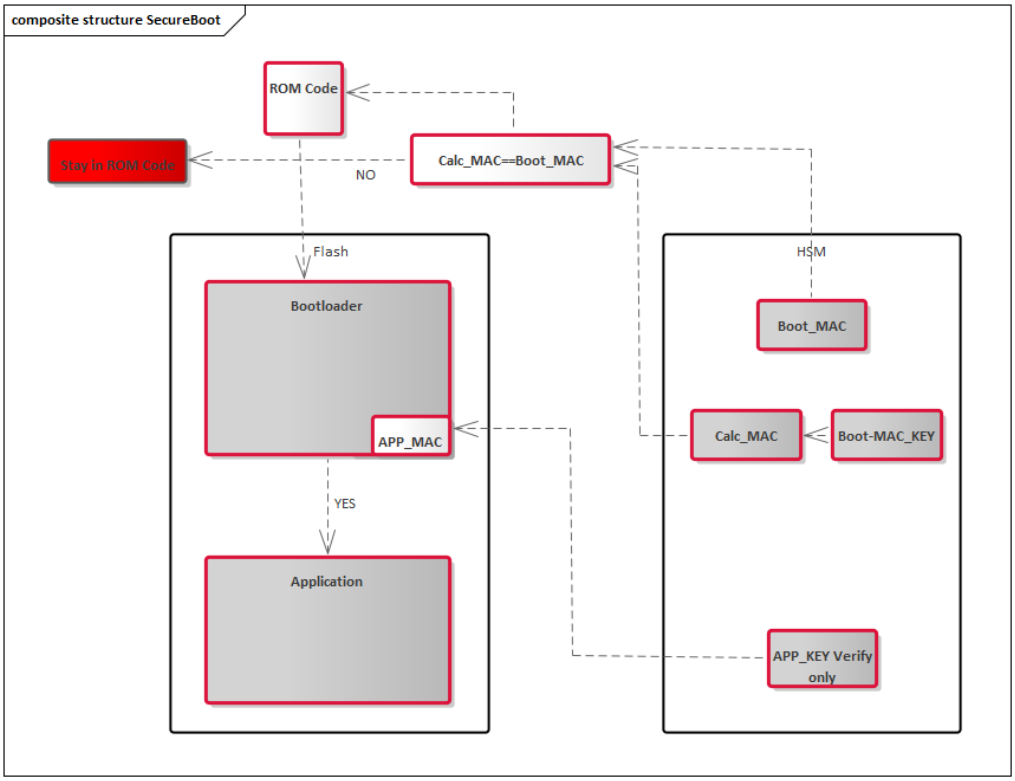


图 2 Secure Boot

- 安全启动信任根

安全启动依赖于芯片硬件支持，用于提供初始信任根的可执行代码和密钥。 信任根密钥用于信任根代码验证已签名软件或已签名的软件关键数据部分内容的第一个启动阶段。 此签名软件用于验证软件组件的后续运行阶段代码。 密钥应该由 OEM 在生产阶段供应给硬件厂商，并存储在受保护内存中。

- 安全启动信任链

安全启动信任链是由信任根代码建立的。通过信任根代码的 root 对第一阶段引导程序进行验证，验证成功则可通过此验证有效的软件执行并继续验证后续引导阶段软件有效性。

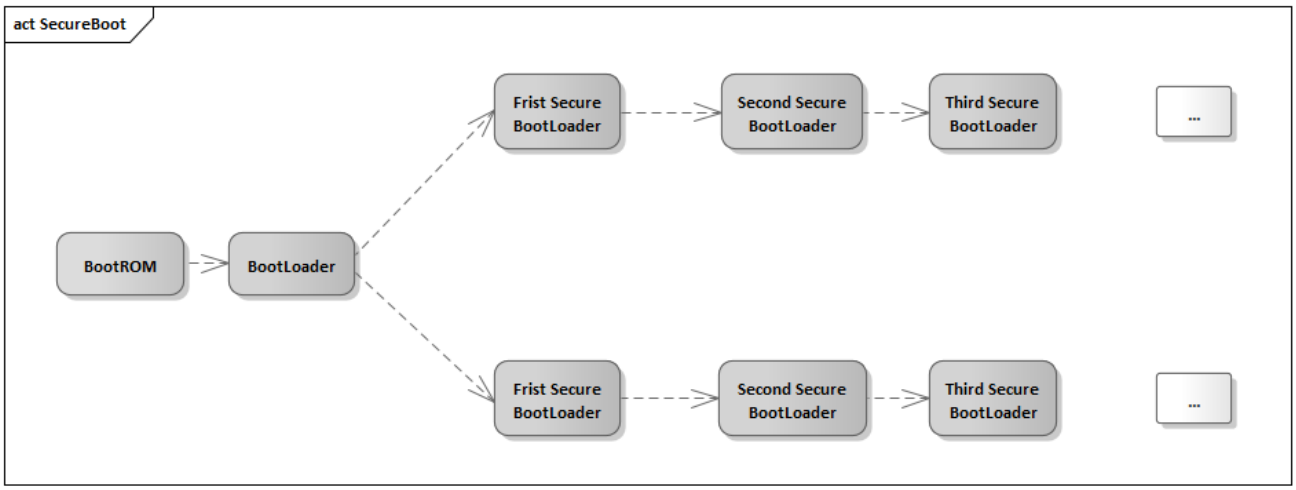


图 3 Secure Boot Routine

- 安全启动过程

通过数据内容加密可实现对数据的保护以防止数据被泄露，同时也可防止数据在传输过程中被篡改。加密算法一般分为对称加密算法和非对称加密算法。对称加密算法的加密和解密使用相同密钥，而非对称算法则使用公钥和私钥加解密数据内容。公钥私钥成对存在，例如用公钥加密需用私钥解密，反之亦然。

AES 是最常用的对称加密算法，其拥有运算速度快，内存需求低，分组长度和密钥长度设计灵活等优点。对于非对称加密算法来说，典型的有 RSA 和 ECC 两种加密算法。RSA 加密算法常被选择用于镜像的签名与验签。

知从科技所开发的木牛 CryptoLibrary 包括硬件加密模块(HSM)的内核固件(zHSM CORE)和客户应用接口函数 (SHE CD)。内核固件除了满足常规的 SHE 功能(密钥注入、对称加解密、消息认证码生成与校验、随机数生成和安全启动等)，还可扩展多种算法，如 HASH 、ECC256 以及国密算法 等。

3 安全诊断 SECUREDIAGNOSTIC

知从科技可以为客户提供 SecureDiagnostic 完整方案，并可针对项目特定需求和硬件模块定制开发，实现的安全诊断特性包括:

- 证书存储解析功能
- 公私钥存储解析功能

- 密钥更新管理功能
- 支持 UDS0x29 服务
- 支持 UDS0x84 服务
- 支持集成信息安全库

安全诊断（SecureDiagnostic）是保护 ECU 内部数据安全的重要手段，主要用于将程序或数据下载 / 上传到服务器以及从服务器读取特定内存位置的诊断服务需要进行身份验证。异常的程序上传或下载到服务器的数据可能会潜在地破坏电子设备或其他车辆部件，或可能违背车辆的排放或安全等标准。另一方面，当从服务器检索数据时，可能会违反数据安全性。因此需在这些服务执行前，要求上位机证明其身份，在合法身份确认之后，才允许其访问数据和诊断服务。

安全诊断是通过某种认证算法来确认客户端的身份，并决定客户端是否被允许访问。可以通过对随机数种子生成的非对称签名进行验证或者通过基于对称加密算法的消息校验码来验证其身份。

知从科技所开发的木牛 CryptoLibrary 支持 X.509v3 证书的解析，认证，存储等流程。可以实现不同 OEM 的规范要求，对证书扩展数据进行解析和处理，可定制开发等。证书在诊断安全认证过程中起到了非常重要的作用，有效避免非法人员窃取控制器数据。

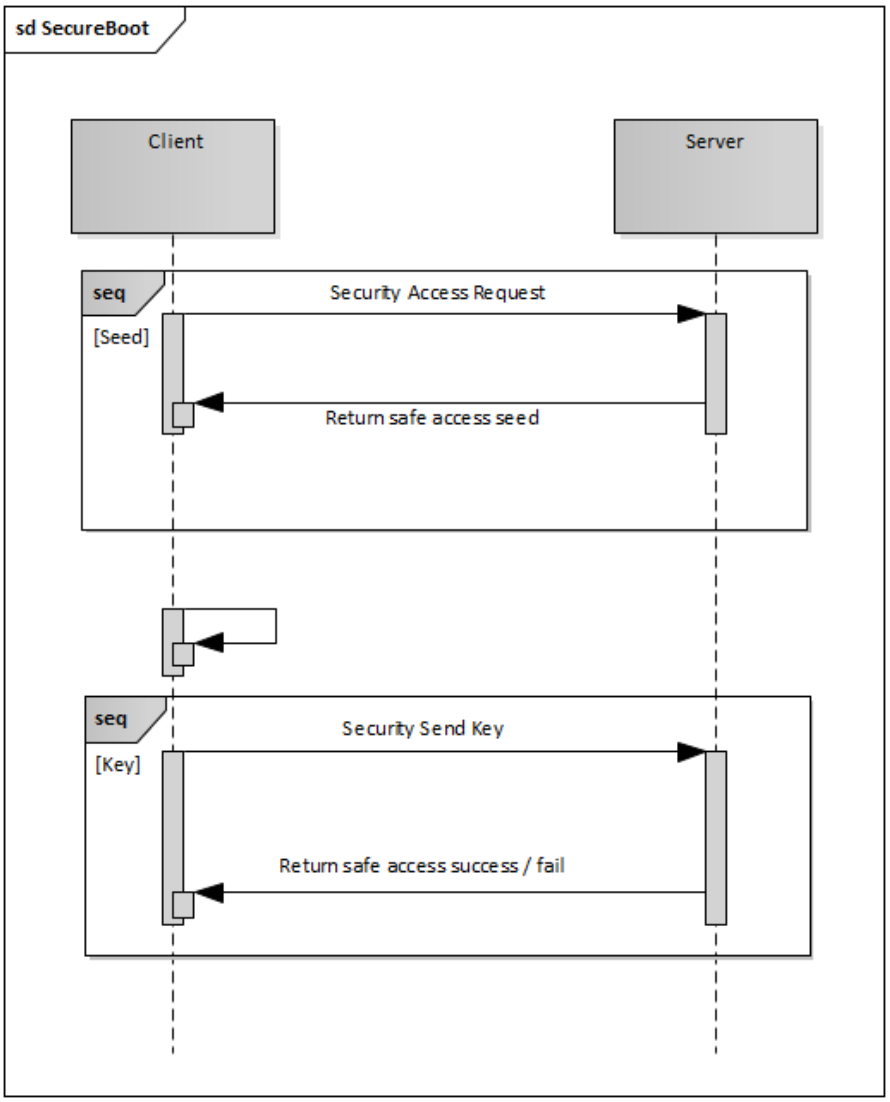


图 4 Secure Diagnostic

4 安全升级 SECUREUPDATE

知从科技可以为客户提供 SecureUpdate 完整方案，并可针对项目特定需求和硬件模块定制开发，实现安全升级特性包括:

- X.509 证书授权管理
- A/B 区备份升级
- 数据压缩下载
- 数据加密升级
- 配套上位机工具(玄武上位机工具)
- 支持不同 OEM 厂家规范

随着越来越复杂的网络环境，在软件升级更新过程中，保证升级包的发布来源有效、不被篡改、数据不丢失以及升级内容不被恶意获取变得越来越重要。

传统升级过程的升级包数据基本上是以明文传输，数据校验方式也是安全性较低的散列算法。安全升级在传统升级基础上，一方面使用添加签名的固件和在固件验证过程中额外执行签名验证来增强固件完整性验证，保证数据来源可靠，数据完整没有被篡改；另一方面还增加了对通过服务器加密固件的解密功能，传输数据过程通过密文传输，有效的降低 OTA 无线更新时数据暴露的风险。

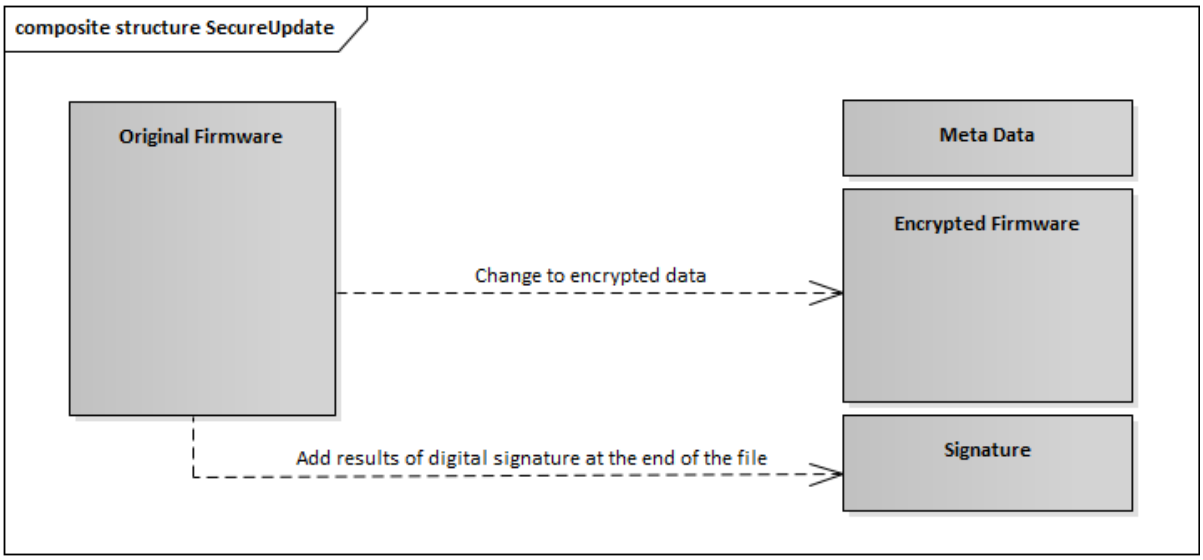


图 5 Secure Update

5 安全日志 SECURELOG

安全日志可以用于记录在安全通信过程中产生的异常问题或授权用户记录等信息，可以方便控制器开发的问题排查以及风险管控。当 ECU 产生信息安全漏洞时，可通过日志信息快速分析影响原因和影响功能，提升代码开发鲁棒性，降低信息安全漏洞导致的一系列影响。

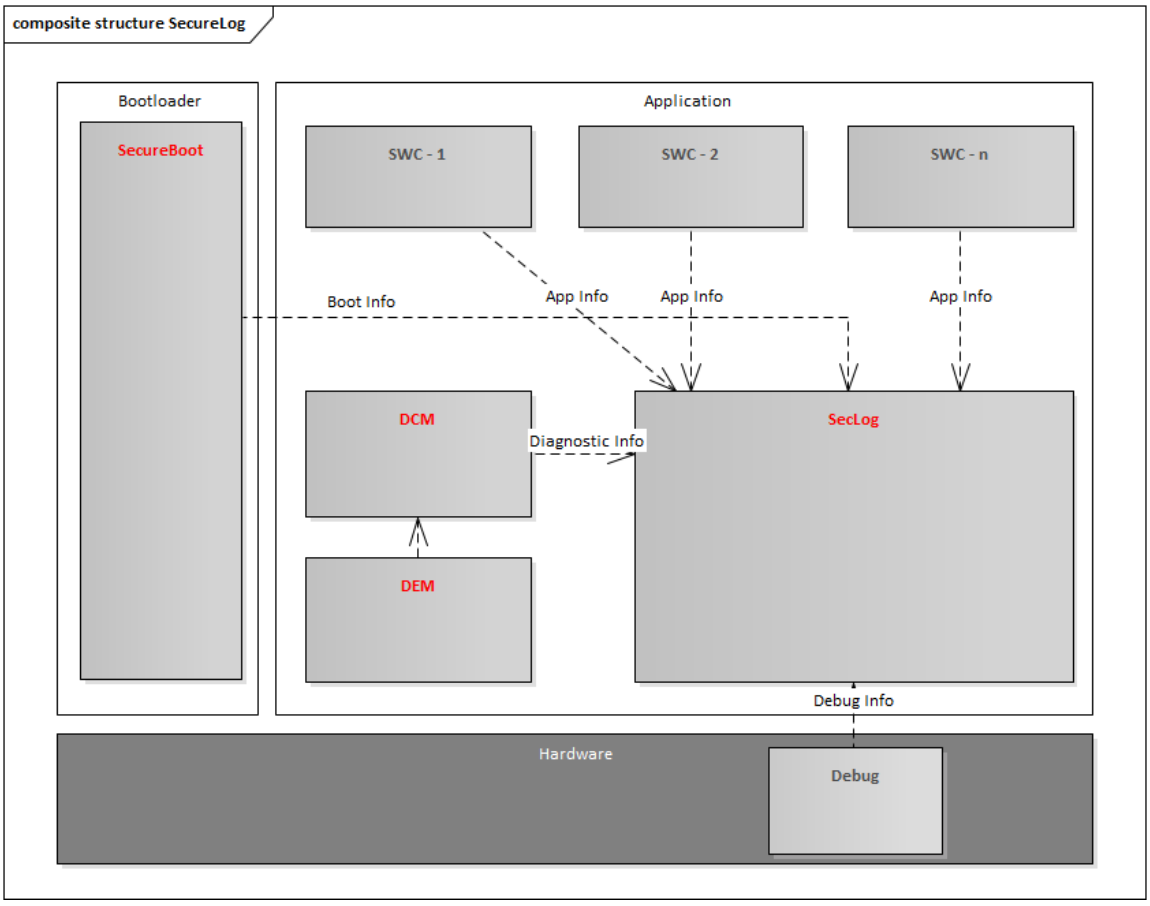


图 6 Secure Log

6 安全通信 SECOC

在目前的车载网络中，大部分数据传输都是在没任何安全措施的情况下进行的。例如应用最广的 CAN 通讯设计之初是没有考虑过信息安全问题的，其明文传输、报文广播传输、极少网络分段等特性，让进入整车网络的黑客如同进了游乐场，轻松便可以伪造报文对车辆进行控制。

SecOC 是在 AUTOSAR 软件包中添加的信息安全组件（组件位置及可应用的通讯方式如下图所示），该 Feature 增加了 CMAC 运算、秘钥管理、新鲜值管理和分发等一系列的功能和新要求。SecOC 模块在 PDU 上为关键数据提供有效可行的身份验证机制，认证机制与当前

的 AUTOSAR 通信系统无缝集成，同时对资源消耗的影响应尽可能小，以便为旧系统提供附加保护。

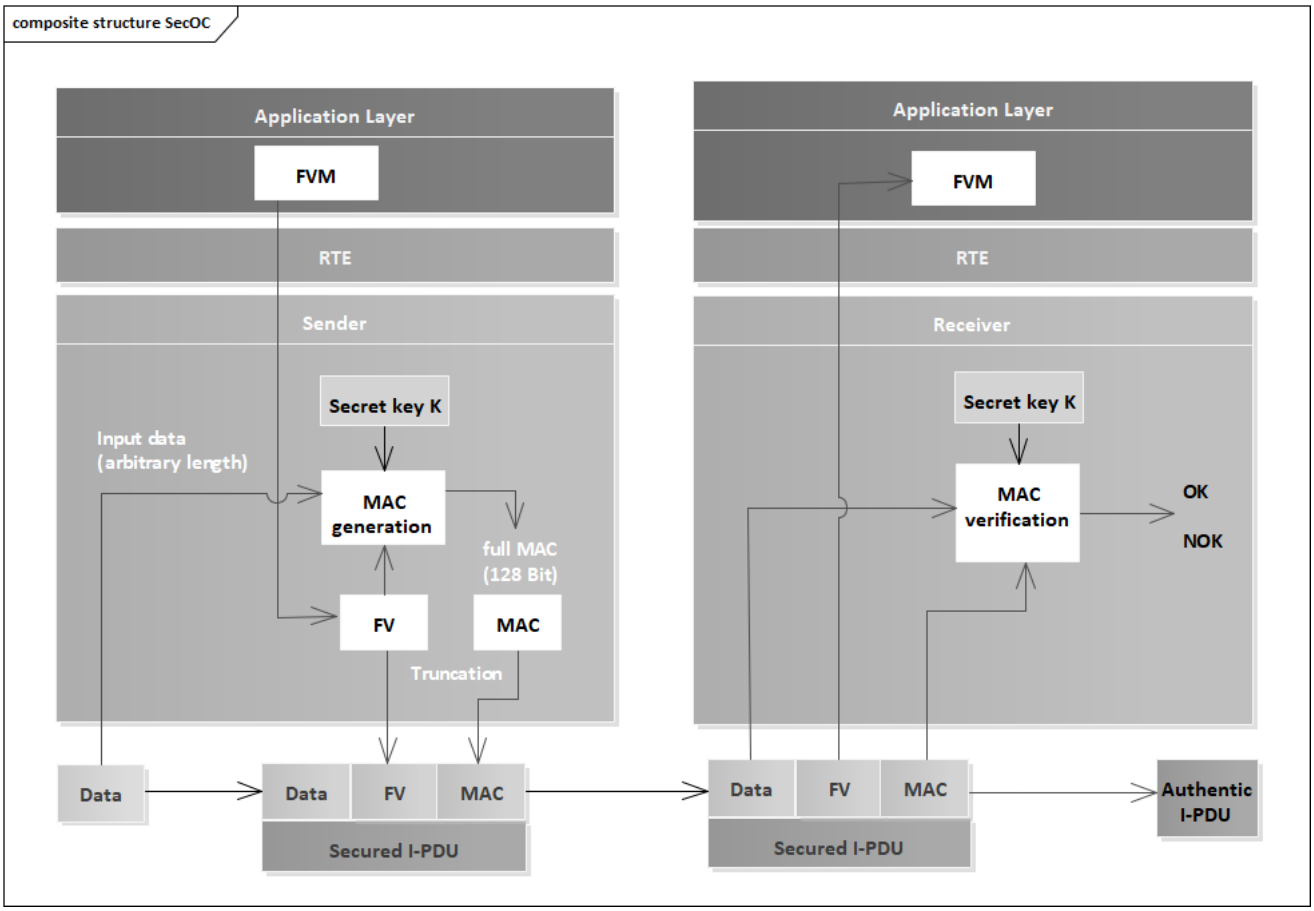


图 7 SecOC

7 安全调试 SECUREDEBUG

知从科技提供的安全调试方案可支持如下内容:

- 下线调试加密流程
- 诊断解密调试权限
- 诊断获取密钥信息

现在大部分控制器都配备了基于硬件的调试功能，用于片上调试过程。安全 JTAG 模式是指通过使用基于 Challenge / Response 的身份验证机制来限制 JTAG 访问。检查对 JTAG 端口的任何访问，只有授权的调试设备（具有正确响应的设备）才能访问 JTAG 端口，未经授权的

JTAG 访问尝试将被拒绝。在生产或者下线阶段，必须要禁用或者锁定相关的调试诊断接口，禁用意味着无法与硬件调试接口建立连接，锁定意味着硬件调试接口受到保护，只能根据安全调试解锁来访问。

知从科技针对不同厂家芯片，制定了不同的安全调试功能方案。例如针对 NXP S32K1xx 系列芯片，可以通过安全诊断方式开启和关闭 Debug 功能，通过 SecureDiagnostic 确保授权用户可执行调试功能。

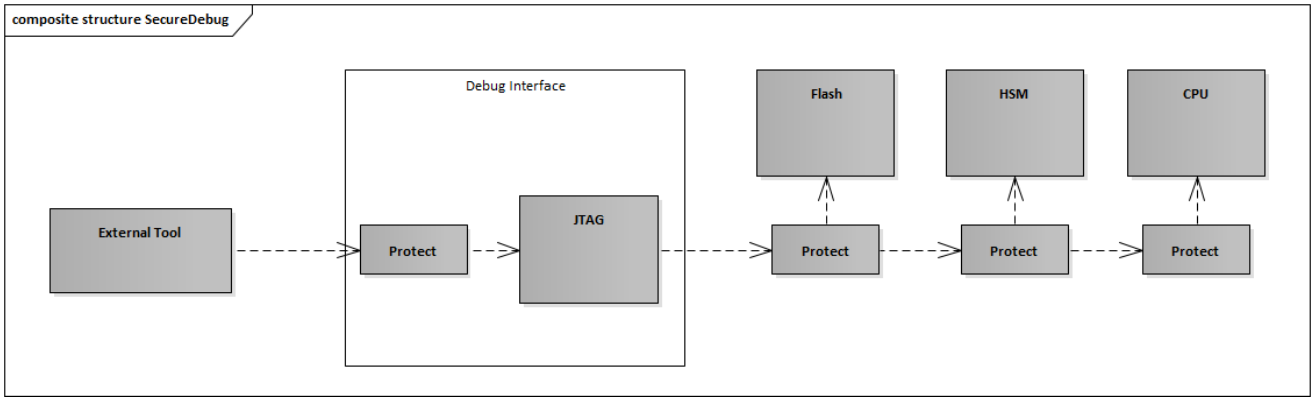


图 8 Secure Debug

8 安全存储 SECURESTORAGE

安全存储可保护数据区域内容不被异常窃取，避免因为控制器通过强行访问数据存储区，将存储的密钥，证书等内容进行复制。目前主流芯片都可通过设置 Flash，Nvm，RAM 等存储区进行数据保护，开启此功能可有效避免上述情况产生。

部分芯片包含加密功能，内部存储的安全数据还可通过地址区域数据加密存储方式进行保护，即便破解了数据访问权限，仍然无法得到明文数据内容。部分芯片也带有一次性可编程存储器 OTP(On Chip One Time Programmable ROM, On-Chip OTP ROM)，也称为 eFuse，是芯片中特殊存储模块，字段中的任何 eFuse 位都只能从 0 编程为 1（融合），只能被烧写一次，但是读取操作没有限制。安全存储还可以通过将 Flash 某些区域设置只读或者只写来实现，防止非法访问和篡改。Flash 保护区域的数量和大小会根据 Flash 的类型和该 Flash 块的大小而有所不同。

9 知从木牛 CRYPTOLIBRARY 信息安全库

知从科技针对英飞凌 TC2xx/TC3xx 系列(如 TC275,TC264,TC39x,TC38x 和 TC37x 等)开发了木牛 CryptoLibrary，包括硬件加密模块(HSM)的内核固件(zHSM CORE)和客户应用接口函数 (SHE CD)。

知从木牛 CryptoLibrary 的软件主要分为两部分：

1) HSM 硬件加密模块固件(zHSM CORE)

2) Tricore 主核的 SHE 复杂驱动(zSHE CD)

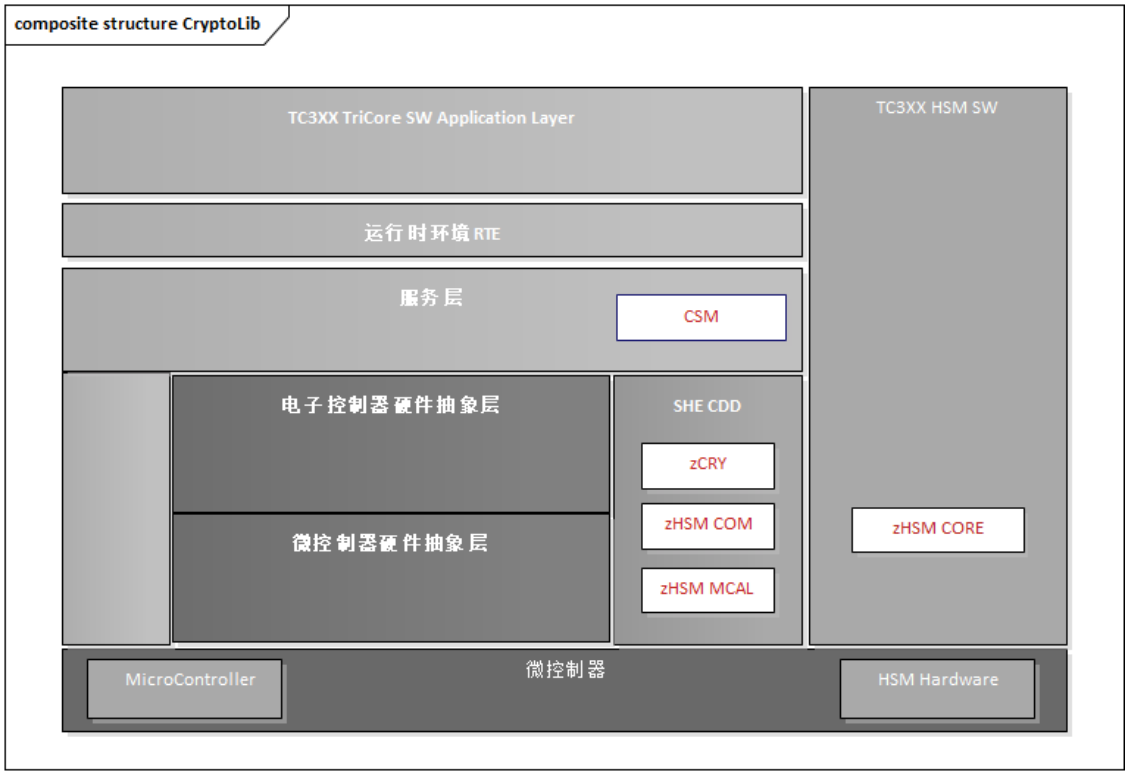


图 9 Crypto Library

zSHE CD 包含和 CSM 的接口 zCRY 模块, 和 HSM 通讯的 zHSM COM 和 zHSM MCAL 模块三个子模块，各模块的功能介绍如表 1。

表 1 软件模块功能说明

软件模块	模块组件	AUTOSAR Layer	功能定义
zHSM CORE (加密内核)	zHSM CORE	N/A	使用了 HSM 内部的硬件加速器，如随机数生成器、AES-128 等（如图 10）

zSHE CD （主核）	1) zCRY 2) zHSM COM 3) zHSM MCAL	SHE CD	微处理器 Hsm 驱动、与 Hsm 核的通信驱动、Crypto Interface 等
CSM （主核）	CSM	SERVICE	用户信息安全管理的接口函数

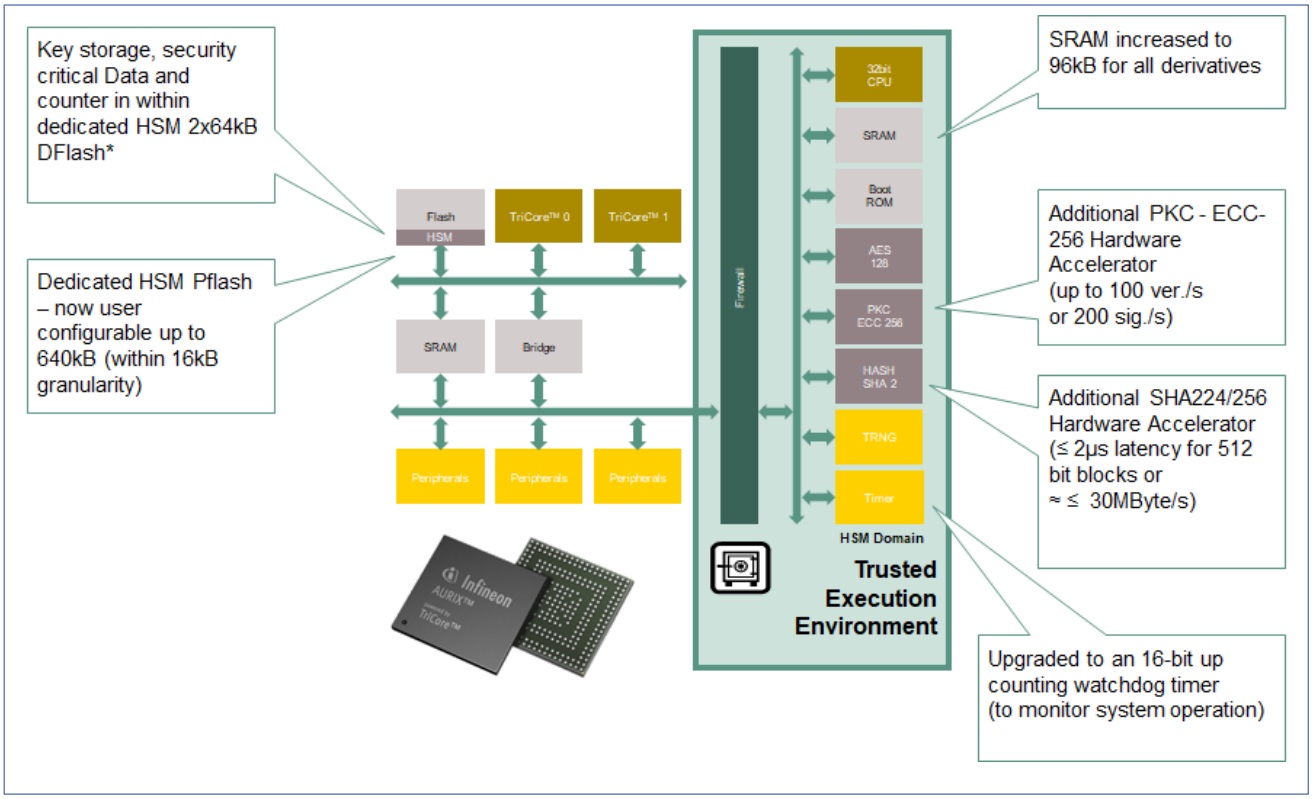


图 10 TC3xx HSM 资源

木牛 CryptoLibrary 支持 SHE 标准，和标准的 SHE 相比，CryptoLibrary 在功能上有一些扩展，主要功能及区别见表 2 和 3。

表 2 木牛 CryptoLibrary(TC3xx)的主要功能

Features		SHE standard	木牛 CryptoLibrary
AES 128 密码模式	ECB	✓	✓

	CBC	✓	✓
AES 128 消息认证码	CMAC	✓	✓
随机数生成器	伪随机数	✓	✓
	硬件随机数	/	✓
安全启动		✓	✓
非易失性密码槽		**10**	**>50**
可易失性密码槽		✓	✓
支持可用于消息认证密钥		/	✓
安全消息认证		/	✓
非对称加密	ECDSA	/	✓
	ED25519	/	✓
	Curve25519 / X25519	/	✓
密钥协商	ECDH	✓	✓
	KDF	✓	✓

X509 证书	证书链校验	/	✓
	根证书替换	/	✓
	OCSP response 校验	/	✓
	公钥私钥存储	/	✓
	Custom Externsion 支持	/	✓
国密算法	SM2	/	✓
	SM3	/	✓
	SM4	/	✓

表 3 木牛 CryptoLibrary 的 SHE 功能说明

主要功能	解释说明
SHE 对称密钥加解密	对称式 AES-128，支持 ECB 和 CBC 加密模式对称加密
SHE CMAC 消息认证码 生成与校验	对称式 AES-128 消息认证码
SHE CMAC 安全消息认证码 生成与校验	支持安全 CMAC 验证，使应用程序能够检查安全相关数据的完整性
SHE 明文密钥装载	存储 128 位密钥到 HSM 的 RAM, 不涉及安全协议
SHE 密钥导出	对导出 RAM 密钥进行包装(加密和身份验证)
SHE 基于安全协议的密钥装载	使用安全协议将 128 位密钥存储在 HSM 非易失性存储器中
SHE 随机数生成	使用 AES 生成伪随机数,种子由 TRNG 生成
SHE 安全启动	验证应用程序启动代码的 CMAC.
SHE 调试模式	使用安全协议启用对 HSM 调试接口的访问
SHE 状态获取	获取 SHE 状态.
SHE 命令取消	取消当前正在执行的操作.
SHE 错误报告	除了 CSM 返回代码之外，还可以通过 AUTOSAR 机制报告 SHE 错误
SHE 超时处理	如果 HSM 响应时间超过预定义的限制，则报告错误
应软件更新支持 (Cipher 和 MAC)	在应用软件的更新过程中也可以使用密码和 MAC 功能
硬件随机数	支持生成真随机数
AES 加密扩展 (OFB, CFB, CTR, XTS,GCM)	支持额外的 AES 模式
密钥扩展	支持扩展更多的非易失性密钥

10 证书

中华人民共和国国家版权局

计算机软件著作权登记证书

证书号：软著登字第6700633号

软件名称：知从木牛信息安全库软件
[简称：信息安全库]
V1.0

著作权人：上海知从科技有限公司

开发完成日期：2020年03月14日

首次发表日期：2020年06月03日

权利取得方式：原始取得

权利范围：全部权利

登记号：2020SR1895504

根据《计算机软件保护条例》和《计算机软件著作权登记办法》的规定，经中国版权保护中心审核，对以上事项予以登记。

中华人民共和国国家版权局
计算机软件著作权登记专用章

No. 07119009

2020年12月25日

木牛软件著作权登记证书

上海市软件行业协会

软件产品证书

经评估,知从木牛信息安全库软件[简称：信息安全库]V1.0 符合《进一步鼓励软件产业和集成电路产业发展的若干政策》和《软件产品评估规范》的有关规定，评估为软件产品，特发此证。

申请企业：上海知从科技有限公司
软件类别：应用软件
证书编号：沪ZC-2021-0019
有 效 期：五年

上海市计算机软件评测重点实验室
（上海计算机软件技术开发中心）
二〇二一 年 一 月二十五 日

木牛软件 CYBERSECURITY 产品证书

公众号　业务联系

通过我们的产品和服务,提高汽车电子控制器开发的质量和速度,降低客户成本,增强产品的可维护性。

Our products and services will improve the quality and speed of ECU development, reduce customer costs, and enhance the maintainability of their product.