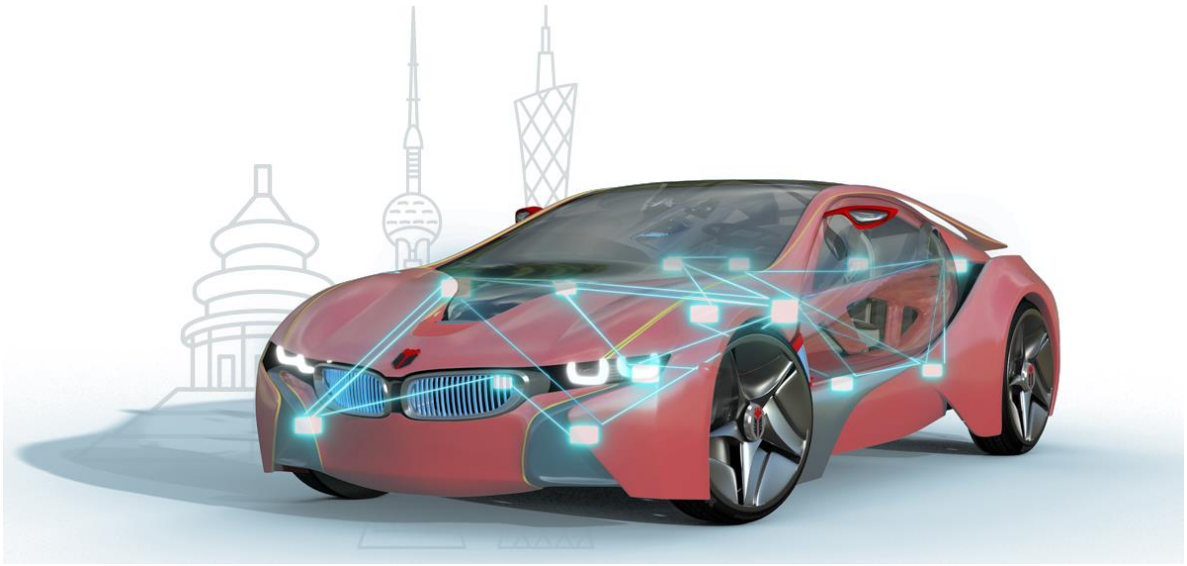
英飞凌 TC2XX 知从木牛信息安全应用介绍

INFINEON TC2XX SECURE APPLICATION INTRODUCTION FROM ZC.MUNIU CYBERSECURITY

知从木牛基础软件平台信息安全库

ZC.MuNiu Basic Software Platform Cybersecurity Library



英飞凌 TC2XX 知从木牛信息安全应用介绍

INFINEON TC2XX SECURE APPLICATION INTRODUCTION FROM ZC.MUNIU CYBERSECURITY

知从木牛基础软件平台信息安全库

ZC.MuNiu Basic Software Platform Cybersecurity Library

1 应用介绍 INTRODUCTION TO THE APPLICATION

早期的汽车是一个比较封闭的系统，不与外界互联。随着汽车向着智能化和网联化的方向发展，信息安全正在占据重要的位置。ISO21434 标准的出台，标志着汽车电子对信息安全的要求也越来越严格，相关需求日益增多。随着中国《汽车整车信息安全技术要求》标准于 2024 年下半年正式推出，进一步细化了汽车信息安全领域的技术规范与实施标准，并且标志着汽车安全领域将进入真正强监管时代。

In the early days, automobiles were relatively closed systems that did not connect with the outside world. As vehicles evolve towards intelligence and connectivity, Cybersecurity is becoming increasingly important. The ISO21434 standard has also been introduced, and the requirements for Cybersecurity in automotive electronics are becoming stricter, with growing demands. With the formal launch of China's “Technical Requirements for Vehicle Cybersecurity” standard in the second half of 2024, the technical specifications and implementation standards in the field of vehicle Cybersecurity have been further refined, and it marks that the field of Cybersecurity will enter an era of real strong regulation.

MCU 端的信息安全是汽车整车信息安全体系中的重要环节：

Cybersecurity on the MCU side is a crucial part of the overall vehicle Cybersecurity system:

- 安全启动（SecureBoot）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，可以有效防止攻击者恶意篡改软件；
  Secure Boot verifies the integrity and authenticity of key programs in user-defined Flash, effectively preventing attackers from maliciously tampering with software.
- 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；
  Secure Diagnostic ensures that application data cannot be accessed by third parties, preventing information leaks.
- 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，可有效避免非官方程序被控制器执行；
  Secure Update ensures that only authorized software can be used by the controller, and when paired with Secure Boot, it can effectively prevent the execution of unofficial programs by the controller.
- 安全通信（SecOC）可有效确保通信数据安全，防止行车过程中通信数据被攻击篡改导致危险事故；
  Secure Communication (SecOC) can effectively ensure the security of communication data, preventing data tampering during driving that could lead to dangerous accidents
- 安全调试（SecureDebug）防止控制器内部安全数据被非法导出修改；
  Secure Debug prevents illegal export and modification of internal security data in the controller.
- 安全存储（SecureStorage）避免控制器数据内部数据被非法软件获取；
  Secure Storage prevents illegal software from accessing internal data of the controller.
- 安全日志（SecureLog）可以有效记录控制器产生的异常数据，并且防止控制器被异常篡改和信息窃取，保护控制器的信息安全。
  Secure Log can effectively record abnormal data generated by the controller and prevent the controller from being tampered with or information being stolen, protecting the controller's Cybersecurity.

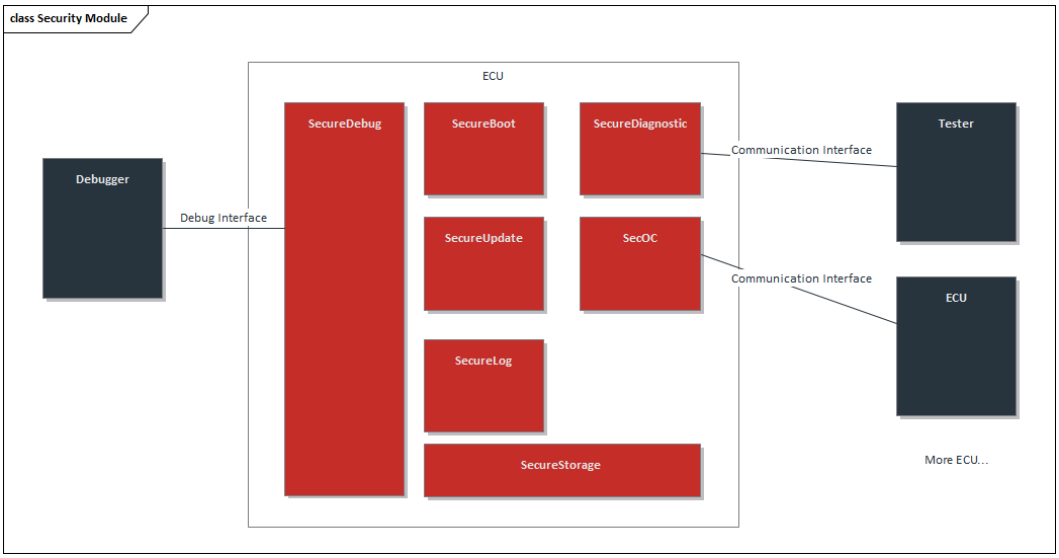


FIGURE1 ECU SECURITY MODULE

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:

ZC can provide customers with a complete Secure Boot solution and can customize development for specific project requirements and hardware modules:

- 基于硬件加密方案
  Based on hardware encryption solutions
- 基于软件加密方案
  Based on software encryption solutions
- 密钥存储管理方案
  Key storage management solutions
- 安全启动失效分析
  Secure boot failure analysis
- 产线生产模式方案
  Production line manufacturing mode solutions

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。

Secure Boot is a fundamental function of the MCU, implemented through hardware encryption modules. This mechanism must operate independently of user programs and cannot be compromised. As the foundation of the entire secure boot trust chain, Secure Boot is mainly used to verify the integrity and authenticity of key programs defined by users in Flash memory after the MCU starts and before user programs execute, to determine if they have been tampered with. If the verification fails, it indicates that the MCU is in an untrusted state, and some functions or even the entire program cannot run.

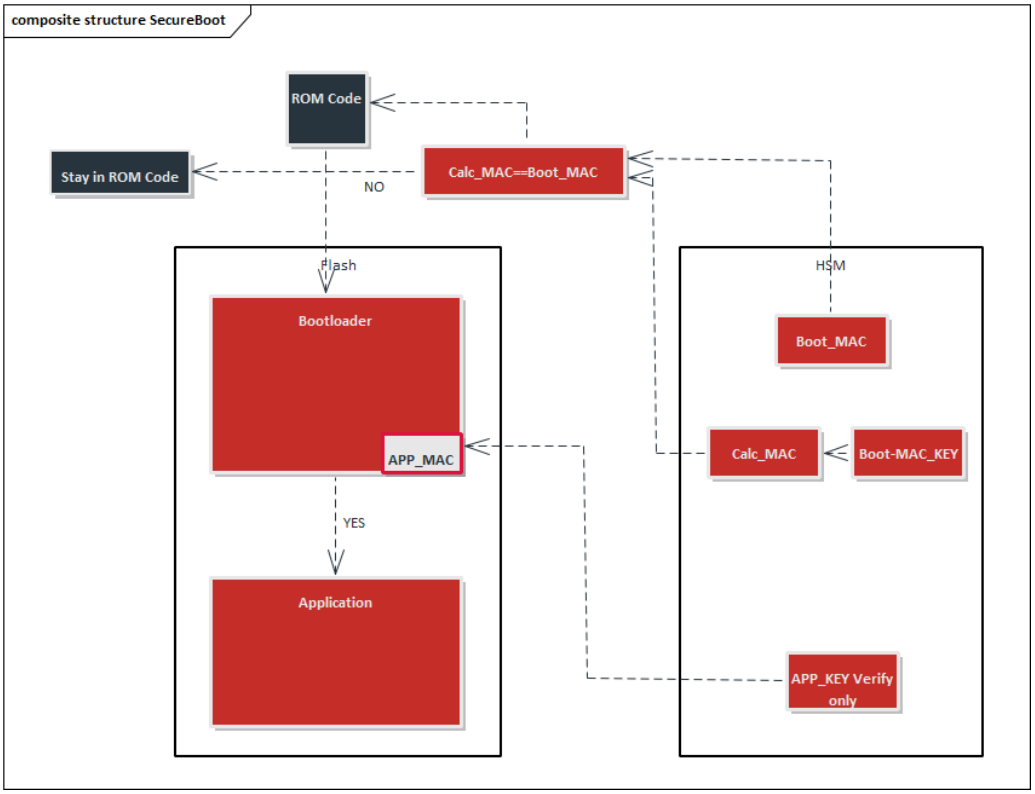


FIGURE 2 SECURE BOOT

➢ 安全启动信任根 Secure Boot Root of Trust

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。

Secure Boot relies on chip hardware support to provide executable code and keys for the initial trust root. The trust root key is used by the trust root code to verify the first stage of signed software or signed key data parts of the software. This signed software is used to verify the subsequent stages of software component code. The key should be supplied by the OEM to the hardware manufacturer during the production phase and stored in protected memory.

➢ 安全启动信任链 Secure Boot Chain of Trust

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。

The Secure Boot trust chain is established by the trust root code. By verifying the first stage bootloader through the root of the trust root code, if the verification is successful, the valid software can execute and continue to verify the validity of subsequent boot stages.

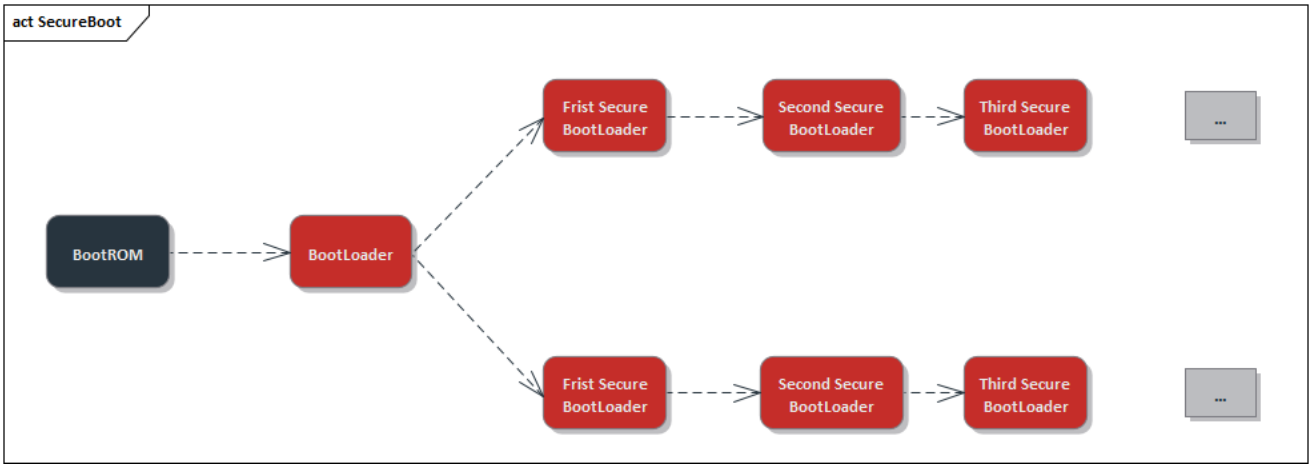


FIGURE 3 SECURE BOOT ROUTINE

➢ 安全启动过程 Secure Boot Process

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。

Data content encryption can achieve data protection to prevent data leakage and also prevent data from being tampered with during transmission. Encryption algorithms are generally divided into symmetric encryption algorithms and asymmetric encryption algorithms. Symmetric encryption algorithms use the same key for encryption and decryption, while asymmetric algorithms use public and private keys to encrypt and decrypt data content. Public and private keys exist in pairs; for example, data encrypted with a public key must be decrypted with a private key, and vice versa.

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。这两种加密算法常被选择用于用户所定义的 Flash 区域的签名与验签。

AES is the most commonly used symmetric encryption algorithm, with the advantages of fast computation speed, low memory requirements, and flexible design of block length and key length. For asymmetric encryption algorithms, the typical ones are RSA and ECC. These two encryption algorithms are often chosen for signing and verification of user-defined Flash areas.

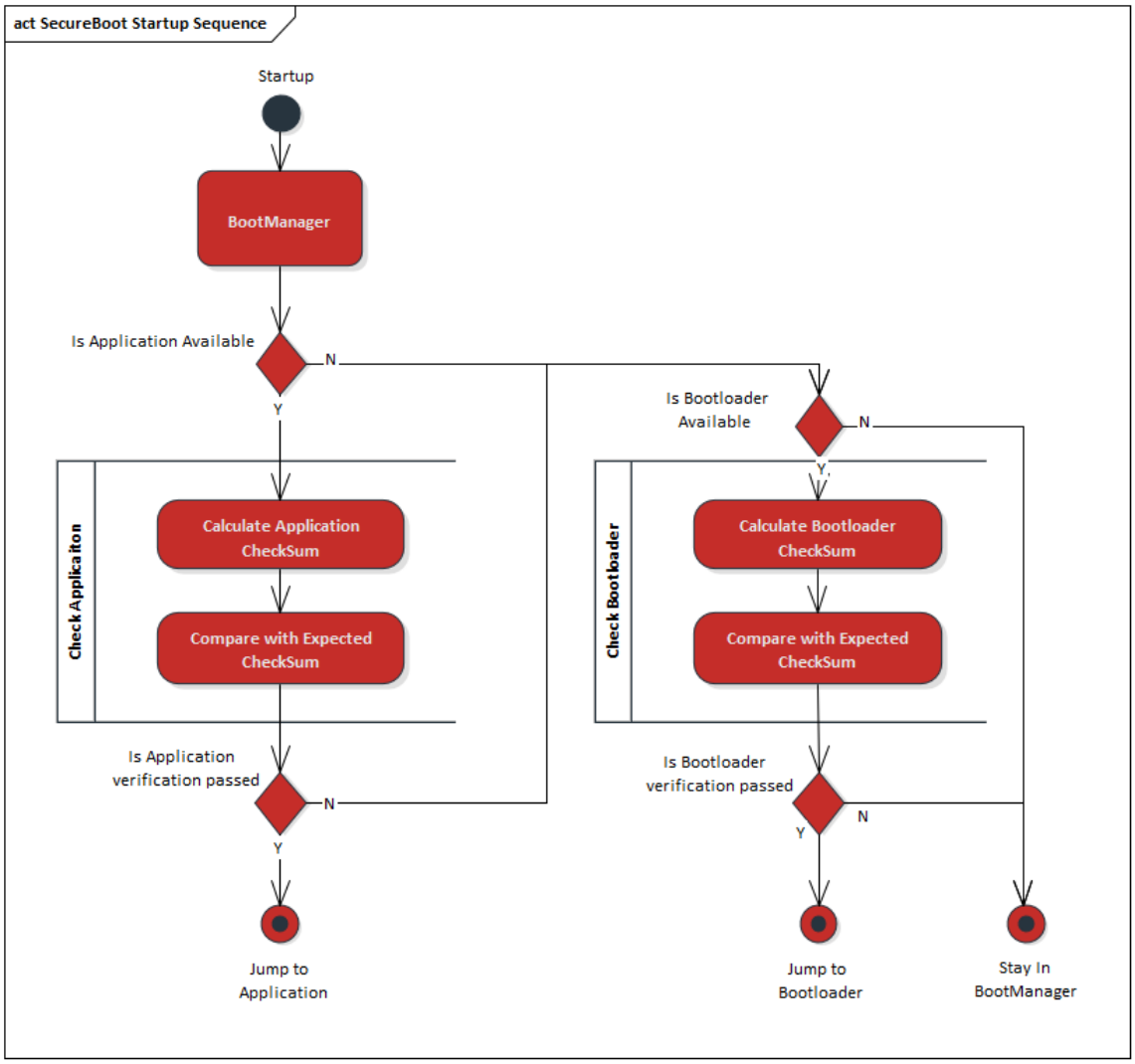


FIGURE 4 SECURE BOOT RROCESS

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)，主核的加密协议栈 CryptoStack（CSM、CRYIF、CRYPTO、KEYM）以及 HSM CDD(zHSM COM、zHSM CRY)。内核固件除了满足 NIST 主流国际密码算法，如 AES、HASH、ECC 和 TRNG/DRNG 等，并且包含国密算法 SM2/3/4，还可扩展多种基于算法的功能：对称加解密、非对称签名生成与解签、安全启动、安全刷写和 SecOC 等。 CryptoStack 和 HSM CDD 除了满足支持 AUTOSAR 4.4.0 的版本需求外，还可以作为一个单独的复杂驱动，在非 AUTOSAR 环境集成。

The ZC.MuNiu CryptoLibrary developed by ZC includes the core firmware of the hardware encryption module (HSM) (zHSM CORE), the main core encryption protocol stack CryptoStack (CSM, CRYIF, CRYPTO, KEYM), and HSM CDD (zHSM COM, zHSM CRY). The core firmware not only meets NIST mainstream international cryptographic algorithms such as AES, HASH, ECC, and TRNG/DRNG but also includes national cryptographic algorithms SM2/3/4, and can expand various functions based on algorithms: symmetric encryption and decryption, asymmetric signature generation and signature verification, secure boot, secure flashing, and SecOC.

CryptoStack and HSM CDD, in addition to meeting the needs of AUTOSAR 4.4.0 version support, can also be integrated as a separate complex driver in non-AUTOSAR environments.

3 安全诊断 SECURE DIAGNOSTIC

知从科技可以为客户提供安全诊断完整方案，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：

ZC can provide customers with a complete Secure Diagnostic solution and can customize development for specific project requirements and hardware modules. The secure diagnostic features implemented include:

- 证书存储解析功能
  Certificate storage and parsing functionality
- 公私钥存储解析功能
  Public and private key storage and parsing functionality
- 密钥更新管理功能
  Key update management functionality
- 支持 UDS0x29 服务
  Support for UDS 0x29 service
- 支持 UDS0x84 服务
  Support for UDS 0x84 service
- 支持集成信息安全库
  Support for integrating Cybersecurity libraries

安全诊断（Secure Diagnostic）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。

Secure Diagnostic is an important means of protecting the internal data security of ECUs (Electronic Control Units). It is primarily used for diagnostic services that require identity verification when programs or data are downloaded/upload to a server and when specific memory locations are read from the server. Unusual program uploads or downloads to the server could potentially damage electronic devices or other vehicle components, or may violate vehicle emission or safety standards. On the other hand, when retrieving data from the server, data security could be compromised. Therefore, it is necessary to require the upper computer to prove its identity before executing these services, and only after legal identity confirmation is allowed to access data and diagnostic services.

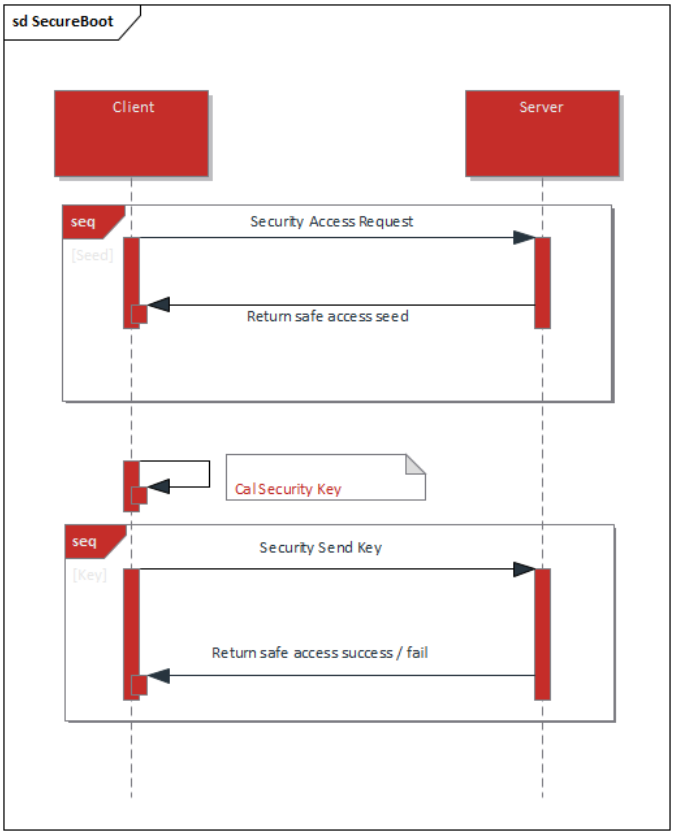


FIGURE 5 SECURE DIAGNOSTIC

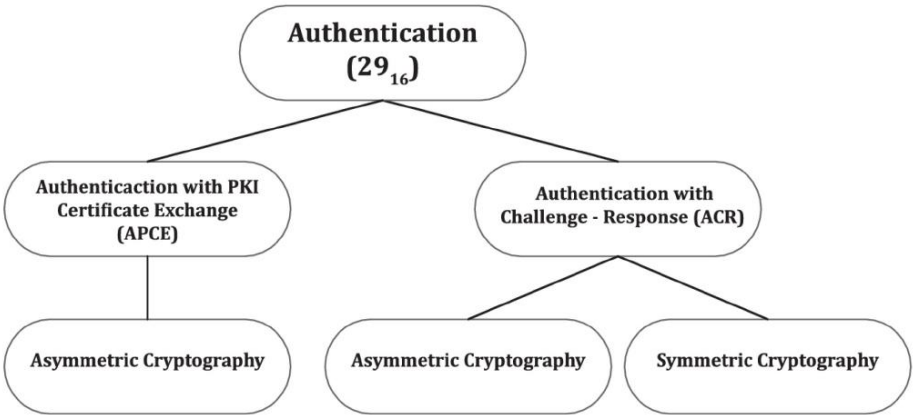
安全诊断是通过某种认证算法来确认客户端的身份，并决定客户端是否被允许访问。可以通过对随机数种子生成的非对称签名进行验证或者通过基于对称加密算法的消息校验码来验证其身份。

Secure diagnostics confirms the identity of the client through some authentication algorithm and decides whether the client is allowed to access. This can be done by verifying the asymmetric signature generated from a random number seed or by verifying the identity through a message authentication code based on symmetric encryption algorithms.

知从木牛 CryptoLibrary 支持的 UDS 0x29 服务，基于 ISO14229-1:2020 标准；其中支持以下两种安全概念：

ZC.MuNiu CryptoLibrary supports the UDS 0x29 service, which is based on the ISO14229-1:2020 standard. It supports the following two security concepts:

- 基于使用非对称密码的 PKI 证书交换过程。
  A PKI (Public Key Infrastructure) certificate exchange process that uses asymmetric cryptography.
- 基于不带 PKI 证书的挑战 - 应答过程，使用带有软件身份验证令牌或对称密码的非对称加密算法。
  A challenge-response process without a PKI certificate, using an asymmetric encryption algorithm with a software authentication token or symmetric cryptography.



知从木牛 CryptoLibrary 支持 0x29 子服务列表：

ZC.MuNiu CryptoLibrary supports the following UDS 0x29 sub-services:

子服务 Sub-service	名称 Name	描述 Description
00	deAuthenticate	此子服务有效地结束认证状态。 This sub-service effectively ends the authentication state.
01	verifyCertificateUnidirectional	此子服务启动单向身份认证验证过程。 This sub-service initiates a unidirectional identity authentication process.
02	verifyCertificateBidirectional	此子服务启动双向身份认证验证过程。 This sub-service initiates a bidirectional identity authentication process.
03	proofOfOwnership	此子服务用于将所有权证明数据传输到诊断仪。 This sub-service is used to transmit proof of ownership data to the diagnostic tool.
04	transmitCertificate	此子服务用于证书或证书链传输。 This sub-service is used for the transmission of certificates or certificate chains.
08	authenticationConfiguration	此子服务用于显示 Server 所提供的认证配置 This sub-service is used to display the authentication configuration provided by the Server.

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。

ZC.MuNiu CryptoLibrary developed by ZC supports the parsing, authentication, and storage of X.509v3 certificates. It can meet the specification requirements of different OEMs, parse and process certificate extension data, and is customizable. Certificates play a very important role in

the diagnostic security authentication process, effectively preventing unauthorized personnel from stealing controller data.

4 安全升级 SECURE UPDATE

知从科技可以为客户提供 Secure Update 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：

ZC can provide customers with a complete Secure Update solution and can customize development for specific project requirements and hardware modules, implementing secure upgrade features including:

- X.509 证书授权管理
  X.509 certificate authorization management
- A/B 区备份升级
  A/B partition backup upgrades
- APP 数据压缩下载
  APP data compressed downloading
- APP 数据安全升级
  APP data secure upgrading
- 配套上位机工具(玄武上位机工具)
  Supporting PCTools (ZC.XuanWu PCTools)
- 支持不同 OEM 厂家规范
  Supporting different OEM manufacturer specifications

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。

As network environments become increasingly complex, ensuring that the release source of upgrade packages is valid, not tampered with, data is not lost, and upgrade content is not maliciously obtained during the software upgrade process is becoming more and more important.

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。

In traditional upgrade processes, the upgrade package data is essentially transmitted in plaintext, and the data verification method is also a less secure hash algorithm.

知从木牛 CryptoLibrary 支持的安全升级在传统升级基础上，一方面使用非对称加密算法如 RSA、ECC 等，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。

The secure upgrade supported by ZC.MuNiu CryptoLibrary, based on traditional upgrades, on the one hand, uses asymmetric encryption algorithms such as RSA, ECC, etc., to add signed firmware and perform additional signature verification during the firmware verification process

to enhance firmware integrity verification, ensuring that the data source is reliable and the data is complete and has not been tampered with. On the other hand, it also adds the decryption function of firmware encrypted by the server, and the transmission process uses encrypted data transmission, effectively reducing the risk of data exposure during OTA wireless updates.

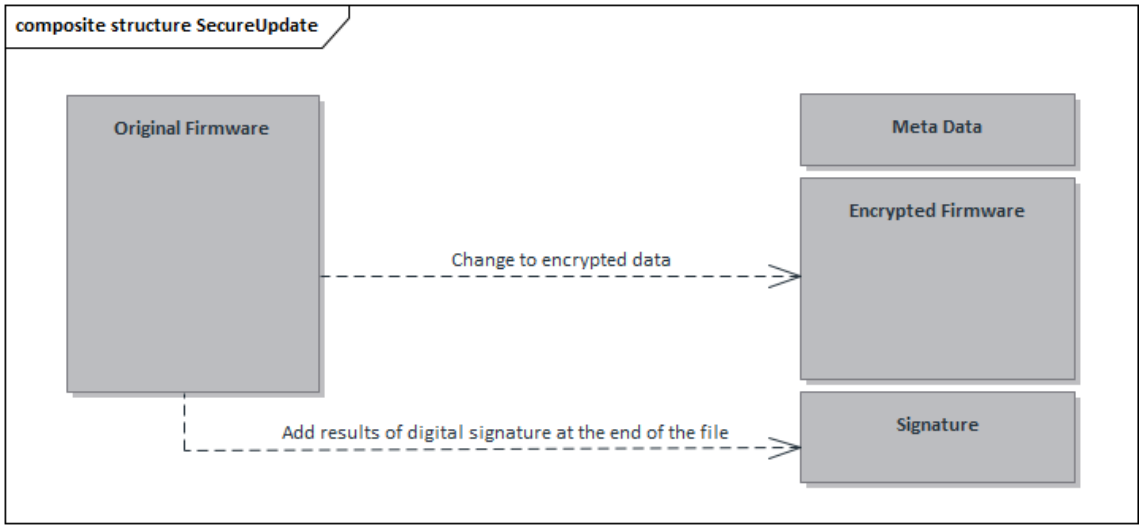


FIGURE 6 SECURE UPDATE

此外，知从木牛 CryptoLibrary 也支持基于证书的安全升级，为用户提供了一种更灵活而安全的方式来更新其车辆的固件。通过使用数字证书进行身份验证，确保只有经过授权的更新才能被安装，从而有效防止了恶意软件的入侵和未授权访问。并且，该库还集成了多种加密算法和安全通信 SecOC，保证数据在传输过程中的机密性和完整性。

Additionally, ZC.MuNiu CryptoLibrary also supports certificate-based secure upgrades, providing users with a more flexible and secure way to update their vehicle's firmware. By using digital certificates for authentication, it ensures that only authorized updates can be installed, effectively preventing the intrusion of malicious software and unauthorized access. Moreover, the library integrates a variety of encryption algorithms and secure communication SecOC, ensuring the confidentiality and integrity of data during transmission.

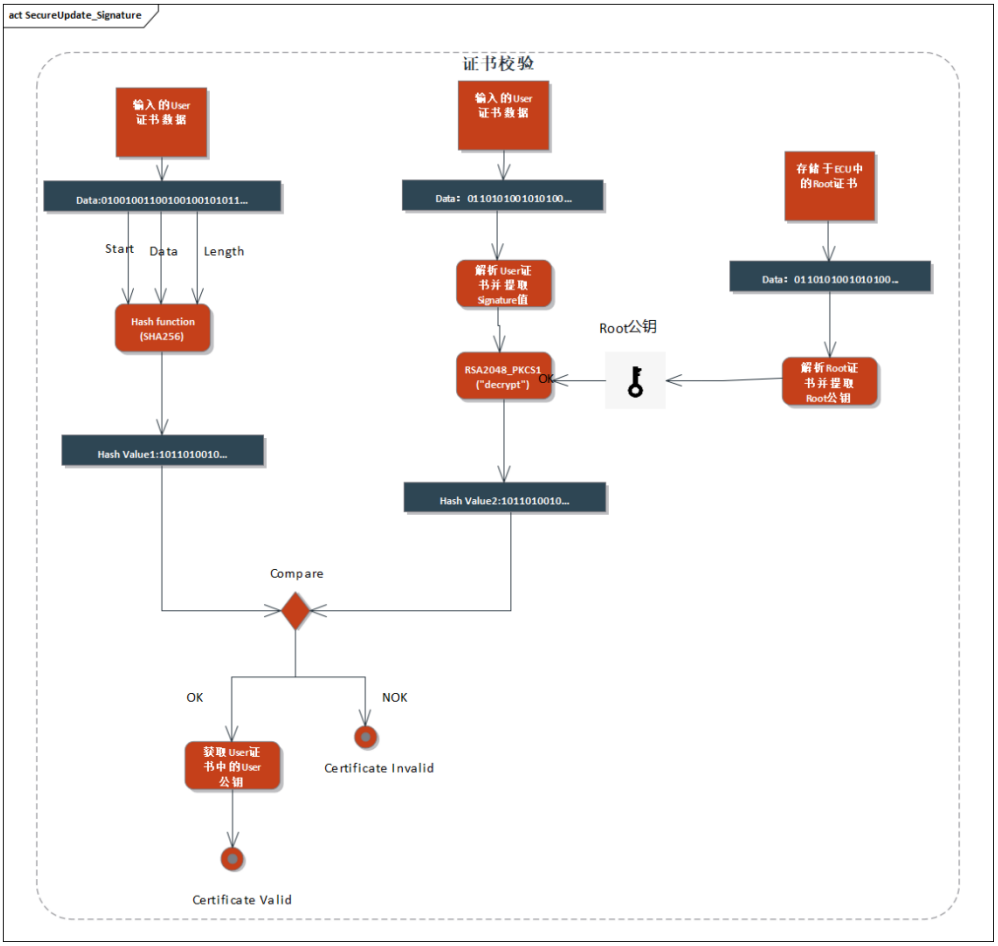


FIGURE 7 SECURE UPDATE WITH CERTIFICATE

5 安全日志 SECURE LOG

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。

Security logs can be used to record anomalies or authorized user records that occur during secure communication processes, facilitating problem diagnosis and risk management in controller development. When an ECU has a Cybersecurity vulnerability, log information can be used to quickly analyze the cause and impact of the vulnerability, enhancing the robustness of code development and reducing a series of impacts caused by Cybersecurity vulnerabilities.

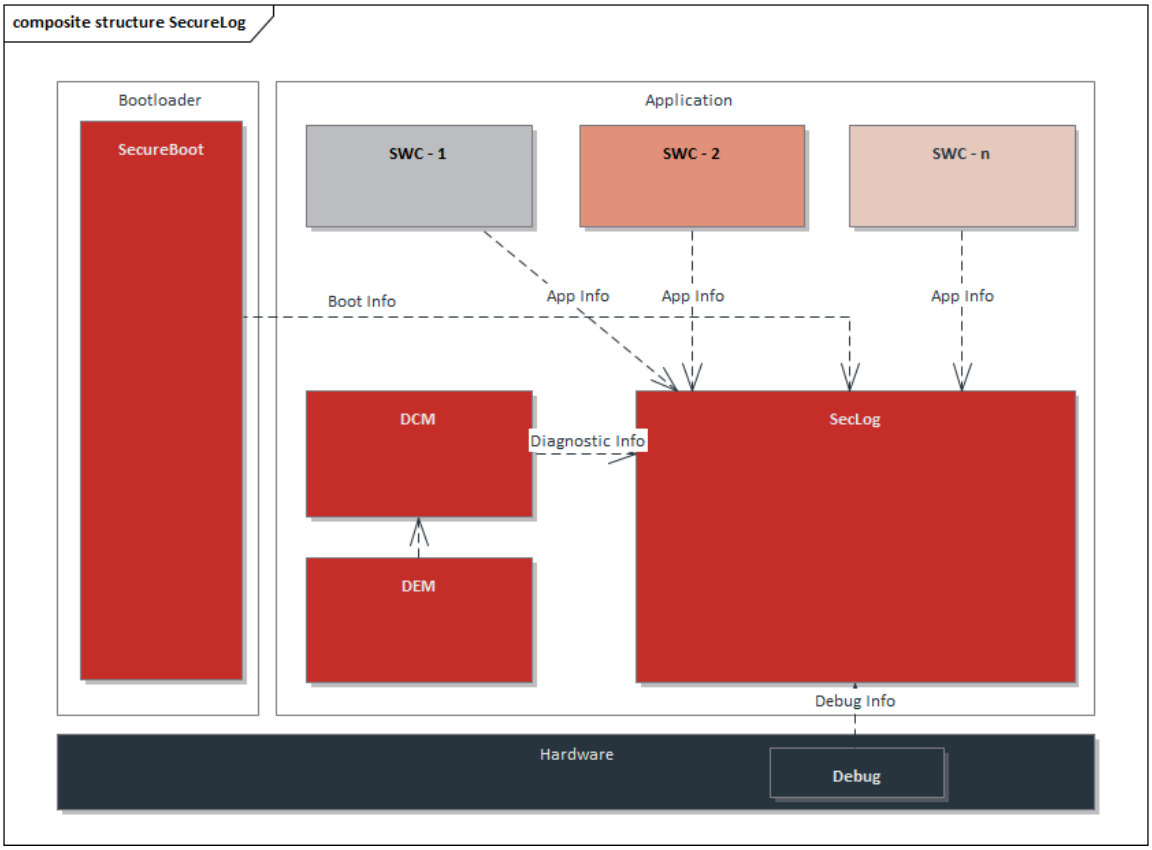


FIGURE 8 SECURE LOG

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。

In the current in-vehicle network, most data transmissions are carried out without any security measures. For example, the widely used CAN communication was not designed with Cybersecurity in mind initially. Its characteristics of plaintext transmission, message broadcasting, and minimal network segmentation make it easy for hackers who enter the vehicle network to control the vehicle by fabricating messages as if they were in an amusement park.

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。

SecOC is a Cybersecurity component added to the AUTOSAR software package (the component location and applicable communication methods are shown in the figure below). This feature adds a series of functions and new requirements such as CMAC calculation, key management, freshness value management, and distribution. The SecOC module provides a viable authentication mechanism for critical data on the PDU, integrating the authentication mechanism seamlessly with the current AUTOSAR communication system, while minimizing the impact on resource consumption to provide additional protection for legacy systems.

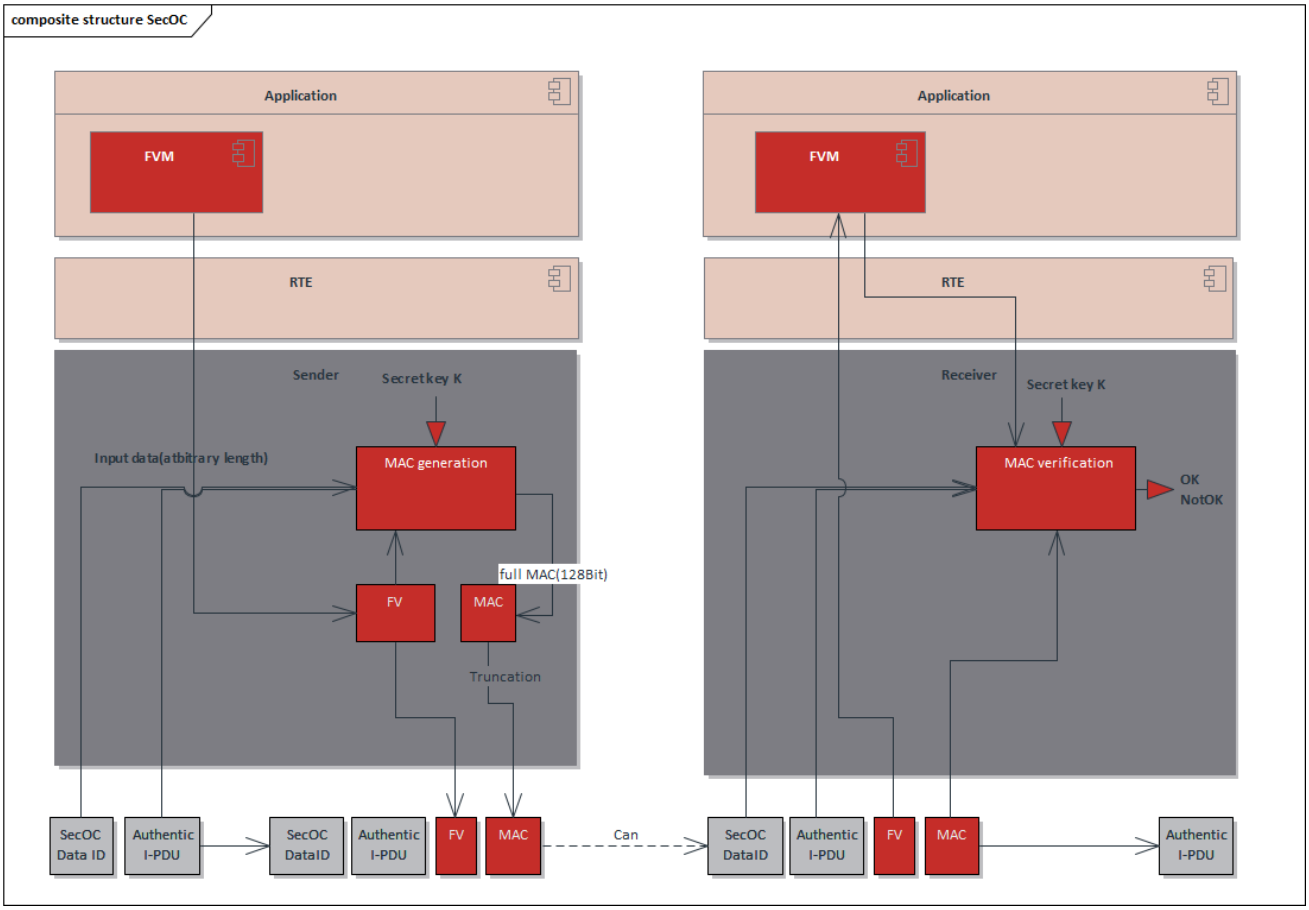


FIGURE 9 SECOC

7 安全调试 SECURE DEBUG

知从科技提供的安全调试方案可支持如下内容：

ZC offers a secure debug solution that supports the following features:

- 下线调试加密流程
  Offline debugging encryption process
- 诊断解密调试权限
  Diagnostic decryption of debugging permissions
- 诊断获取密钥信息
  Diagnostic retrieval of key information

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。

Most controllers nowadays are equipped with hardware-based debugging functions for on-chip debugging processes. Secure JTAG mode refers to the use of a Challenge/Response-based authentication mechanism to restrict JTAG access. Any access to the JTAG port is checked, and only authorized debugging devices (those with the correct response) can access the JTAG port; unauthorized JTAG access attempts will be denied. During production or the offline phase, it is necessary to disable or lock the related debugging diagnostic interfaces. Disabling means that no connection can be established with the hardware debugging interface, while locking means that the hardware debugging interface is protected and can only be accessed through secure debugging unlock.

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。针对 Infineon TC2XX 系列芯片，可以通过将密钥计算接口集成到启动代码中，在 ECU 上电时调用密钥派生接口，通过不同的 ECU serial number 派生出不同的 Derived Key 并进行实时注入，以此开启 Secure Debug 功能。

ZC has developed different secure debugging feature plans for chips from various manufacturers. For Infineon TC2XX series chips, the key calculation interface can be integrated into the startup code, and the key derivation interface is called when the ECU powers up. Different Derived Keys are derived from different ECU serial numbers and injected in real-time to enable the Secure Debug function.

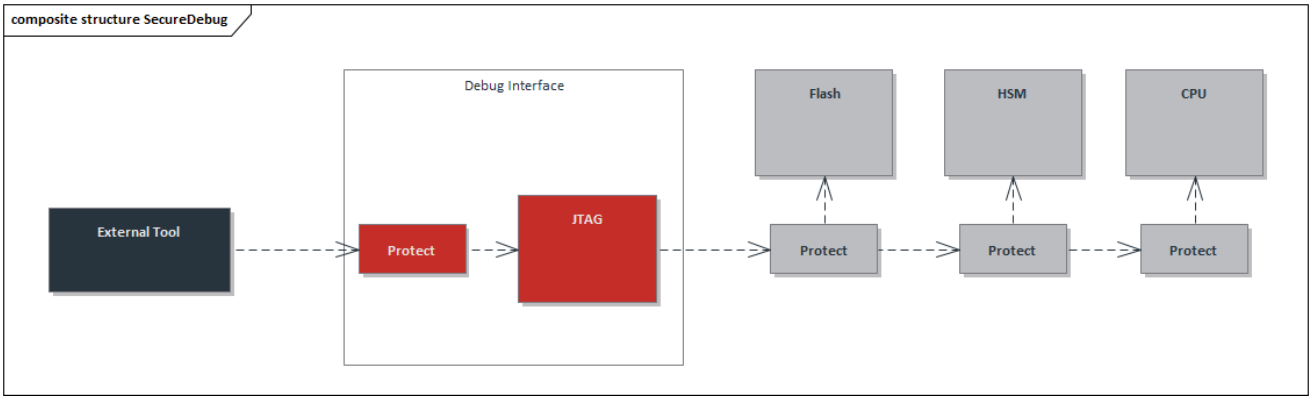


FIGURE 10 SECURE DEBUG

8 安全存储 SECURE STORAGE

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。

Secure Storage can protect the contents of data areas from being stolen abnormally, preventing the copying of stored keys, certificates, and other content due to forced access to the data storage area by controllers. Currently, mainstream chips can protect data by setting up Flash, Nvm, RAM, and other storage areas. Activating this feature can effectively prevent the aforementioned situations.

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。

Some chips include encryption functions, and the secure data stored internally can also be protected by encrypting the data in specific address areas. Even if data access permissions are cracked, the plaintext data content cannot be obtained. Some chips also have one-time programmable memory OTP (On Chip One Time Programmable ROM, On-Chip OTP ROM), also known as eFuse, which is a special storage module in the chip. Any eFuse bit in the field can only be programmed from 0 to 1 (fused) and can only be written once, but there are no restrictions on read operations. Secure Storage can also be achieved by setting certain areas of Flash to read-only or write-only, preventing illegal access and tampering. The number and size of Flash protection areas vary depending on the type and size of the Flash block.

9 知从木牛信息安全库 ZC.MUNIU CYBERSECURITY LIBRARY

9.1 CryptoStack 加密协议栈 CryptoStack Encryption Protocol Stack

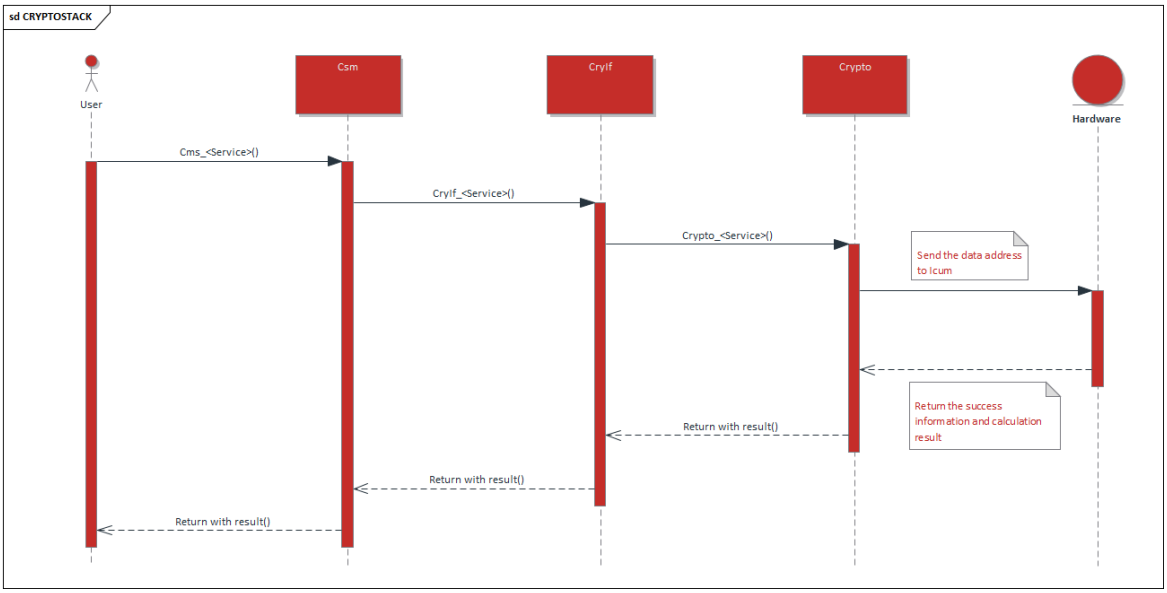


FIGURE 11 CRYPTOSTACK FLOWCHART

知从木牛加密协议栈主要由 Csm、CryIf、Crypto、KeyM 四个模块构成。Csm 模块通过配置 CsmJob 来实现用户所需的信息安全软件或硬件的加密算法需求如 AES-128、CMAC、HASH、TRNG 等，并且提供接口供用户调用。CryIf 模块功能为连接服务层 Csm 模块与硬件抽象层 Crypto 模块，通过加密、解密、校验、认证等安全功能，保护数据的完整性和机密性。Crypto 模块实现主核与 Hsm 加密内核信息数据的传输。KeyM 模块实现密钥与证书的管理，包括对下载进 ECU 的密钥、证书解析校验，连接 HSM 内核驱动将密钥存储进 HSM 受保护区域等功能。

ZC.MuNiu encryption protocol stack is mainly composed of four modules: Csm, CryIf, Crypto, and KeyM. The Csm module implements the encryption algorithm requirements for Cybersecurity software or hardware needed by users, such as AES-128, CMAC, HASH, TRNG, etc., through the configuration of CsmJobs, and provides interfaces for user calls. The CryIf module functions to connect the service layer Csm module with the hardware abstraction layer Crypto module, protecting the integrity and confidentiality of data through security functions such as encryption, decryption, verification, and authentication. The Crypto module implements the transfer of information data between the main core and the Hsm encryption core. The KeyM module implements the management of keys and certificates, including the parsing and verification of keys and certificates downloaded into the ECU, and connecting to the HSM kernel driver to store keys into the HSM protected area.

知从科技针对英飞凌 TC2xx 系列(如 TC275,TC277,TC264 等)开发了木牛 CryptoLibrary，包括硬件加密模块(HSM)的内核固件(zHSM CORE)，主核的 CryptoStack(CSM、CRYIF、CRYPTO、CRYPTO(SW))以及 HSM CDD(zHSM COM、zHSM CRY)。

ZC has developed ZC.MuNiu CryptoLibrary for Infineon TC2xx series (such as TC275, TC277,TC264etc.), including the hardware encryption module (HSM) kernel firmware (zHSM CORE), the main core CryptoStack (CSM, CRYIF, CRYPTO, CRYPTO(SW)), and HSM CDD (zHSM COM, zHSM CRY).

9.2 木牛 CryptoLibrary MuNiu CryptoLibrary

知从木牛 CryptoLibrary 的软件主要分为两部分：

The software of ZC.MuNiu CryptoLibrary is mainly divided into two parts:

1) HSM 硬件加密模块固件(zHSM CORE)

SM Hardware Security Module firmware (zHSM CORE)

2) Trico 主核的 CryptoStack(CSM、CRYIF、CRYPTO、CRYPTO(SW))
以及 HSM/ICUM CDD(zHSM/zICUM COM、zHSM/zICUM CRY)
Trico main core's CryptoStack (CSM, CRYIF, CRYPTO, CRYPTO(SW)) and HSM/ICUM CDD (zHSM/zICUM COM, zHSM/zICUM CRY)

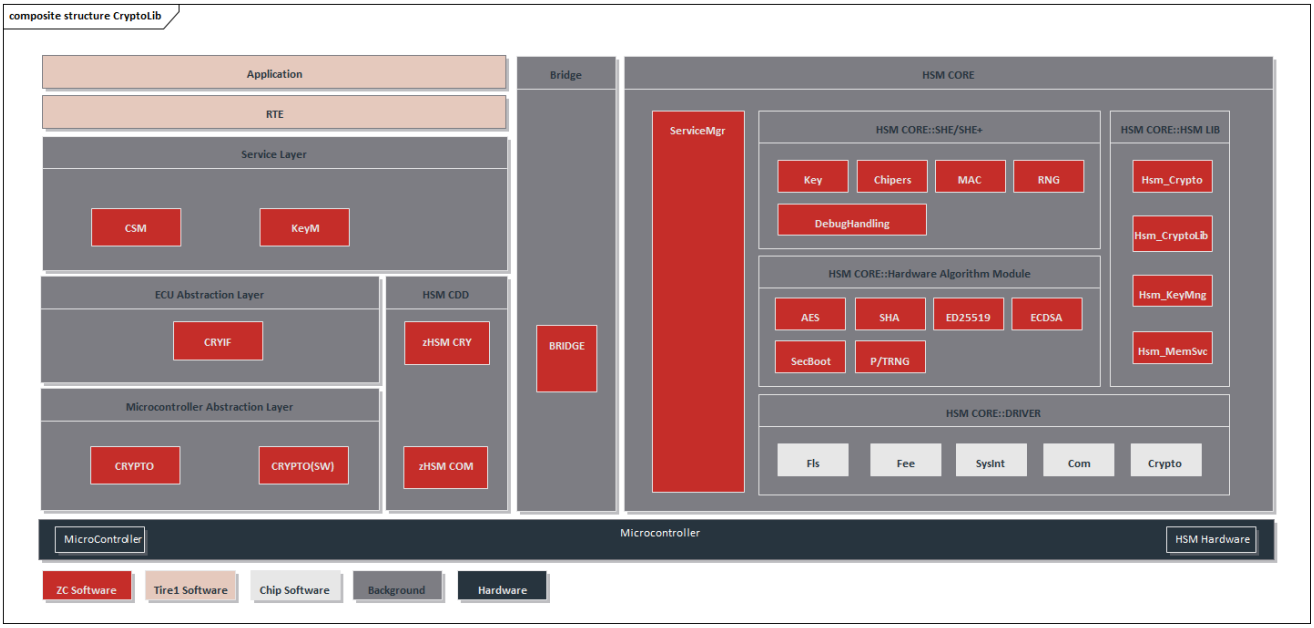


FIGURE 12 CRYPTOLIBRARY BASED ON TC2XX

HSM CDD 包含 Crypto 层调用接口 zHSM CRY 模块和 HSM 通讯的 zHSM COM 模块两个子模块，各模块的功能介绍如表 1。

The HSM CDD includes two sub-modules: the Crypto layer call interface zHSM CRY module and the HSM communication zHSM COM module. The functional description of each module is as shown in Table 1.

表 1 软件模块(TC2XX)功能说明

Table 1 Software Module (TC2XX) Functional Description

软件模块 Software Module	模块组件 Module Component	AUTOSAR 层 AUTOSAR Layer	功能定义 Functional Definition
zHSM CORE (加密内核) (Encryption Core)	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 4） Utilizes HSM's internal hardware accelerators, such as random number generators, AES-128, etc. (as shown in Figure 4)
zHSM CDD （主核） (Main Core)	1) zHSM CRY 2) zHSM COM	CDD	微处理器 HSM 驱动、与 HSM 核的通信驱动、Crypto Interface 等 Microprocessor HSM driver, communication driver with HSM core, Crypto Interface, etc.
CRYPTOSTACK （主核） (Main Core)	1) CSM 2) CRYIF 3) CRYPTO KEYM	SERVICE ECU ABSTRACTION MICROCONTROLLER ABSTRACTION	用户信息安全密钥和 JOB 管理的接口函数，用于配置信息 Interface functions for user Cybersecurity keys and JOB management, used for configuring information

木牛 CryptoLibrary 也支持 SHE 标准，和标准的 SHE 相比，CryptoLibrary 在功能上有一些扩展，包括软件或硬件算法支持，主要功能及区别见表 2 和 3。

ZC.MuNiu CryptoLibrary also supports the SHE (Security Hardware Extension) standard. Compared to the standard SHE, the CryptoLibrary has some functional extensions, including support for software or hardware algorithms. The main functions and differences can be seen in Tables 2 and 3.

表 2 木牛 CryptoLibrary(TC2XX)的主要功能

Table 2 Main Features of MuNiu CryptoLibrary (TC2XX)

Features		SHE standard	ZC.MuNiu CryptoLibrary
AES 128 密码模式 Crypto Mode	ECB	✓	✓
	CBC	✓	✓
	CFB	✓	✓
	OFB	✓	✓
	CTR	✓	✓
	GCM	✓	✓
	XTS	✓	✓
AES 128 消息认证码 Message Authentication Code	CMAC	✓	✓

随机数生成器 Random Number Generator	伪随机数 Pseudo-Random	✓	✓
	真随机数 True Random	✓	✓
安全启动 Secure Boot		✓	✓
非易失性密码槽 Non-Volatile Crypto Slots		23	>50
可易失性密码槽 Volatile Crypto Slots		✓	✓
支持可用于 UDS0x29 认证密钥 Support for UDS0x29 Authentication Keys		／	✓
安全诊断 UDS 0x29 认证 Secure Diagnostic UDS 0x29 Authentication		／	✓
非对称加密 Asymmetric Cryptography	ECDSA*1	／	✓
	RSA*1	／	✓
	ED25519*1	／	✓
密钥协商 Key Agreement	DH*1	／	✓
	ECDH*1	／	✓
	Curve25519 / X25519*1	／	✓

	KDF	✓	✓
密钥存储 Key Storage	RSA 密钥生成[*1] RSA Key Generation	／	✓
	RSA 密钥存储 RSA Key Storage	／	✓
	ECDSA 密钥生成[*1] ECDSA Key Generation	／	✓
	ECDSA 密钥存储[*1] ECDSA Key Storage	／	✓
	Custom Externsion 支持 Custom Extension Support	／	✓
X509 证书 X509 Certificates	证书链校验 Certificate Chain Verification	／	✓
	根证书替换 Root Certificate Replacement	／	✓
	OCSP response 校验 OCSP Response Verification	／	✓
	公钥私钥存储 Public/Private Key Storage	／	✓
	Custom Externsion 支持 Custom Extension Support	／	✓

国密算法 National Cryptography Algorithms	SM2*1	／	✔
	SM3*1	／	✔
	SM4*1	／	✔

注：*1 该算法硬件不支持，支持软件算法

10 证书 CERTIFICATE

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14036127号

软件名称：知从木牛信息安全软件
[简称：知从木牛]
V4.1.0

著作权人：上海知从科技有限公司

权利取得方式：原始取得

权利范围：全部权利

登记号：2024SR1632254

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

2024年10月29日

木牛软件著作权登记证书
MUNIU SOFTWARE COPYRIGHT REGISTRATION CERTIFICATE

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 月二十五日

木牛软件 CYBERSECURITY 产品证书
MUNIU SOFTWARE CYBERSECURITY PRODUCT CERTIFICATE