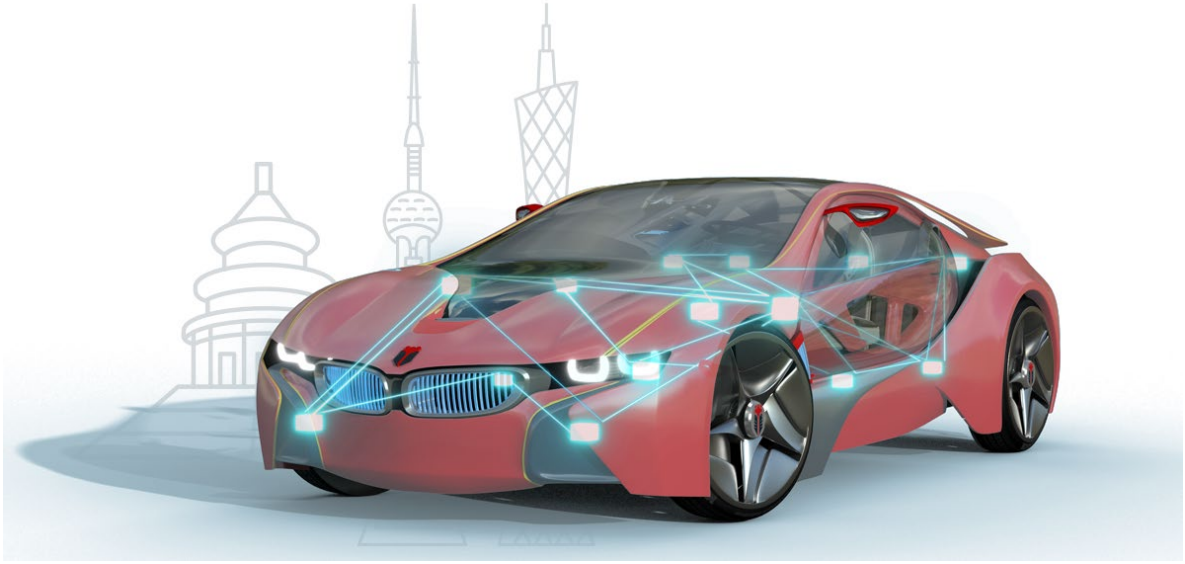
知从木牛恩智浦 S32K1 信息安全服务手册

ZC.MuNiu NXP S32K1 Cybersecurity Security Service Manual

知从工程服务

ZC Project Service



知从木牛恩智浦 S32K1 信息安全服务手册

ZC.MUNIU NXP S32K1 CYBERSECURITY SECURITY SERVICE MANUAL

知从工程服务

ZC Project Service

1 功能概述 INTRODUCTION TO FUNCTION

NXP 提供的 MCAL 信息安全库，包含 Csec 内核驱动 Crypto_Cse 及其配套的 Crypto 模块。

知从基于 NXP 提供的 MCAL 信息安全库，添加了知从木牛信息安全协议栈（CryptoStack）Csm 模块 、CryIf 模块、KeyM 模块，使其与 NXP 内核驱动 Crypto 模块适配，并在此基础上集成了安全通信（SecOC），安全存储（SecureLog）等功能。

The MCAL information security library provided by NXP contains the Csec kernel driver Crypto_Cse and its supporting Crypto modules.

Based on the MCAL cybersecurity library provided by NXP, ZhiCong adds the Csm module, CryIf module and KeyM module of CryptoStack to adapt to the Crypto module of the NXP kernel driver, and integrates SecOC, SecureLog.

- Csm 模块：位于服务层，用来处理用户信息安全任务配置管理与调度
  Csm: Located at the service layer, it is used to handle user information security task configuration management and scheduling.
- CryIf 模块：位于 ECU 抽象层，用于实现 Csm 模块与 Crypto 模块之间的安全通信
  CryIf: located in the ECU abstraction layer, it is used to implement secure communication between the Csm module and the Crypto module.
- KeyM 模块：密钥管理，用来实现密钥与底层 Csec 存储之间的交互
  KeyM module: key management, which is used to realize the interaction between keys and the underlying Csec store.
- 安全通信 SecOC：车载安全通讯，用来保护车辆内 ECU 之间的网络通信，是目前车载网络上一种有效的信息安全方案。

SecOC: In-vehicle Secure Communications, used to protect network communications between ECUs in a vehicle, is currently an effective information security program on in-vehicle networks.

- 安全日志 SecureLog：存储车辆异常状态信息，有效保护控制器在客户端的信息安全
  SecureLog: Stores vehicle abnormal status information to effectively protect the controller's information security on the client side.

知从根据客户需求使用 NXP MCAL 信息安全库进行配置，也可以提供相应的集成测试服务，以满足客户信息安全的工程需求。

ZC uses NXP MCAL information security libraries for configuration according to customer needs, and can also provide appropriate integration testing services to meet customer information security engineering needs.

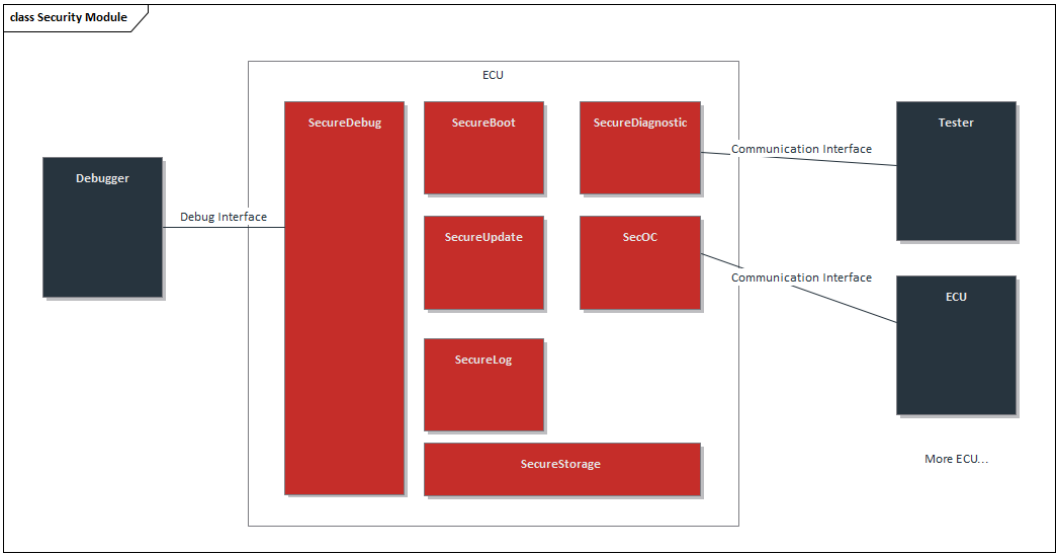


FIGURE1 ECU SECURITY MODULE

2 应用领域 APPLICATION AREAS

基于 NXP 提供的信息安全库并结合知从信息安全协议栈，可应用于有信息安全需求的汽车控制器。例如：

Based on the information security libraries provided by NXP and in combination with the KnowledgeFrom Information Security Protocol Stack, it can be applied to automotive controllers with information security requirements. For example:

- 远程控制器（TBOX）
  Remote Controller (TBOX)
- 车载信息娱乐系统（IVI）
  In-Vehicle Infotainment (IVI)
- 车身控制器(BCM)
  Body Controller (BCM)
- 电动助力转向控制器(EPS)
  Electric Power Steering Controller (EPS)
- 雨刮控制器
  Wiper Controller

通过将信息安全模块集成到汽车电子控制器产品中，除了满足机密性、完整性、可用性等安全基本要素的要求，还具有满足基础软件可裁剪、可配置、实时性等特点的需求。

By integrating the information security module into the automotive electronic controller product, in addition to meeting the requirements of the basic elements of security such as confidentiality, integrity, availability, etc., it also has the ability to meet the needs of the basic software can be cut, configurable, real-time and other characteristics.

3 技术服务 ZC.MUNIU Technical services

3.1 CryptoStack 加密协议栈 CryptoStack Encryption Protocol Stack

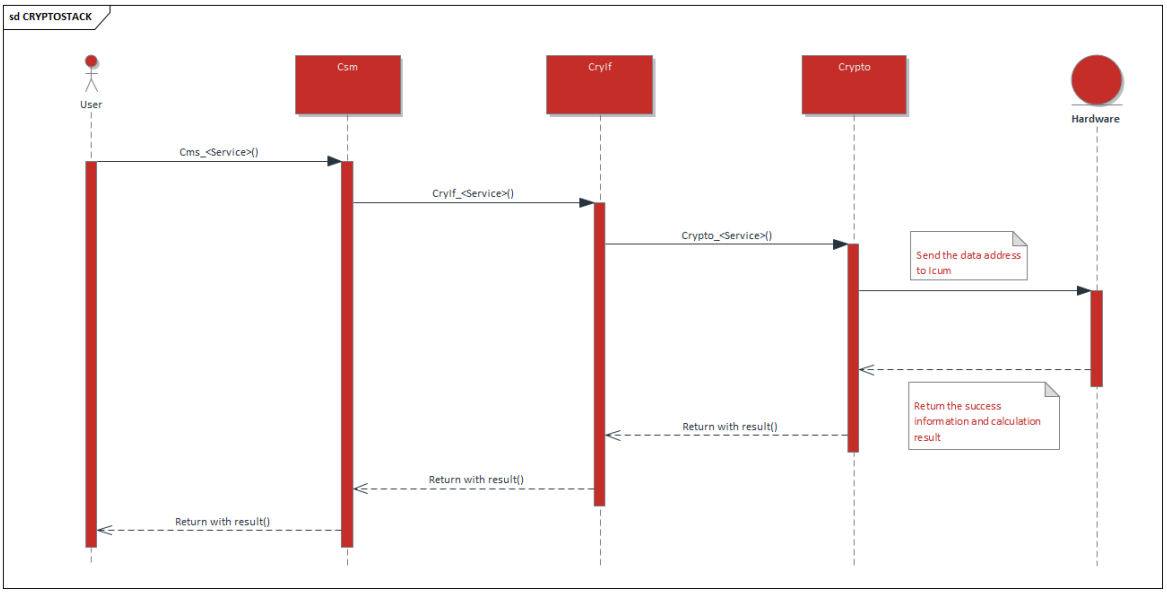


FIGURE 9 CRYPTOSTACK FLOWCHART

知从木牛加密协议栈主要由 Csm、CryIf、KeyM 三个模块构成。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、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。NXP 提供的 Crypto 模块实现主核与 Csec 加密内核信息数据的传输。KeyM 模块实现密钥的管理，包括对下载进 ECU 的密钥，连接 CSEC 内核驱动将密钥存储进 CSEC 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,, 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 provided by NXP implements the transfer of information data between the main core and the Csec encryption core. The KeyM module implements the management of keys, including the parsing and verification of keys and certificates downloaded into the ECU, and connecting to the CSEC kernel driver to store keys into the CSEC protected area.

3.2 安全通信 SecOC

通过配置 SecOC，FvM，PduR 等模块以满足 SecOC 要求；通过配置 Csm，Crylf， Crypto（Csec）等模块来实现 SecOC 认证的加密功能。SecOC 使用 MAC 校验和新鲜度值（FV）对数据进行保护，校验使用 AES-128 的 CMAC 算法生成 MAC 值。在发送时，通过截取 MAC 和 FV 的部分数值来组成 Secured I-PDU，发送给目标 ECU；目标 ECU 接受到 Secured I-PDU 后校验 MAC 值和 FV 值，校验通过则说明该报文数据有效。

SecOC, FvM, PduR and other modules are configured to meet SecOC requirements; Csm, Crylf, Crypto (HW) and other modules are configured to realize the encryption function of SecOC authentication.SecOC protects the data by using MAC checksum and Freshness Value (FV), and checksum generates the MAC value by using the CMAC algorithm of AES-128. When sending, the Secured I-PDU is composed by intercepting some values of MAC and FV, and sent to the target ECU; the target ECU checks the MAC value and FV value after receiving the Secured I-PDU, and if the check passes, it indicates that the message data is valid.

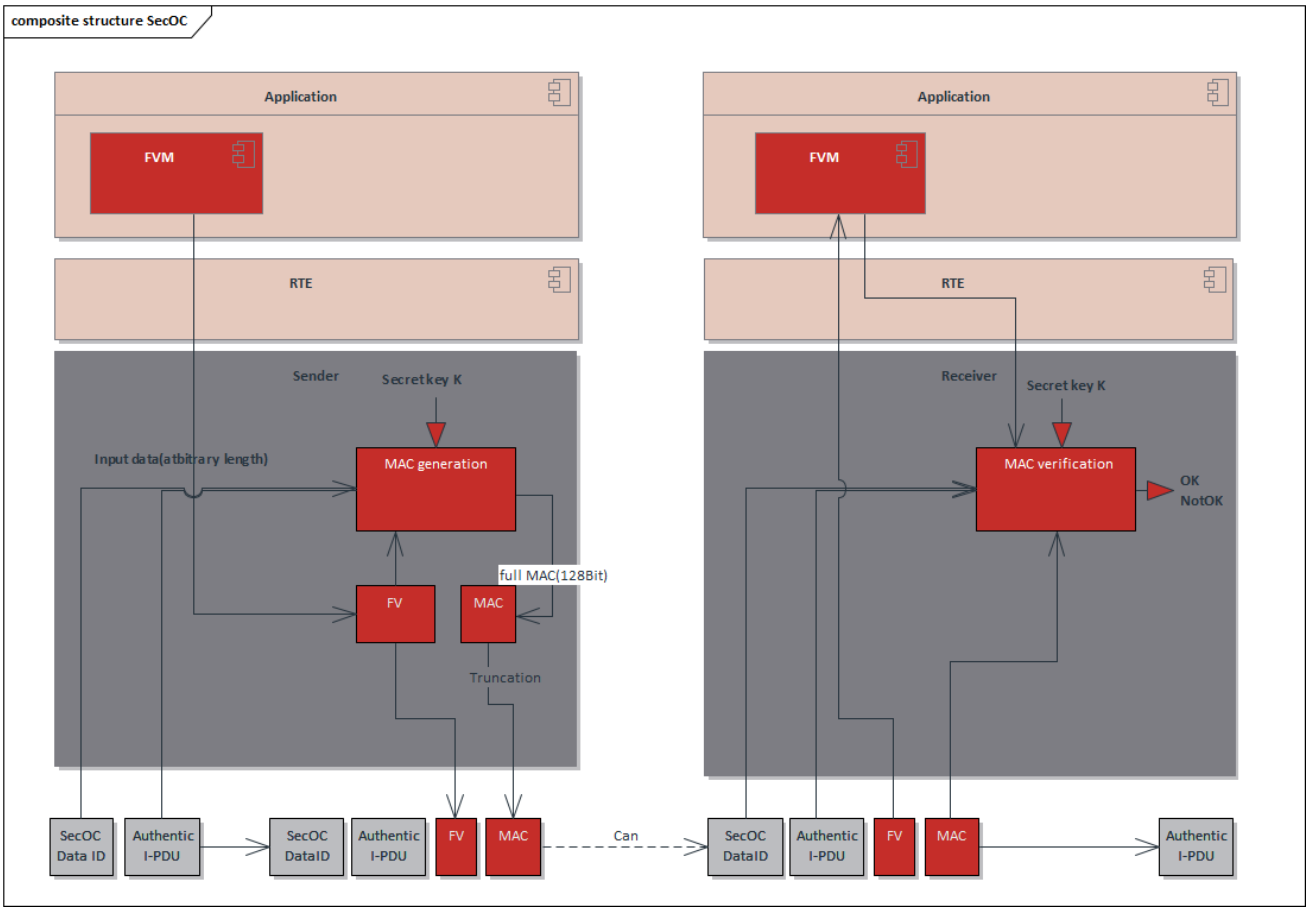
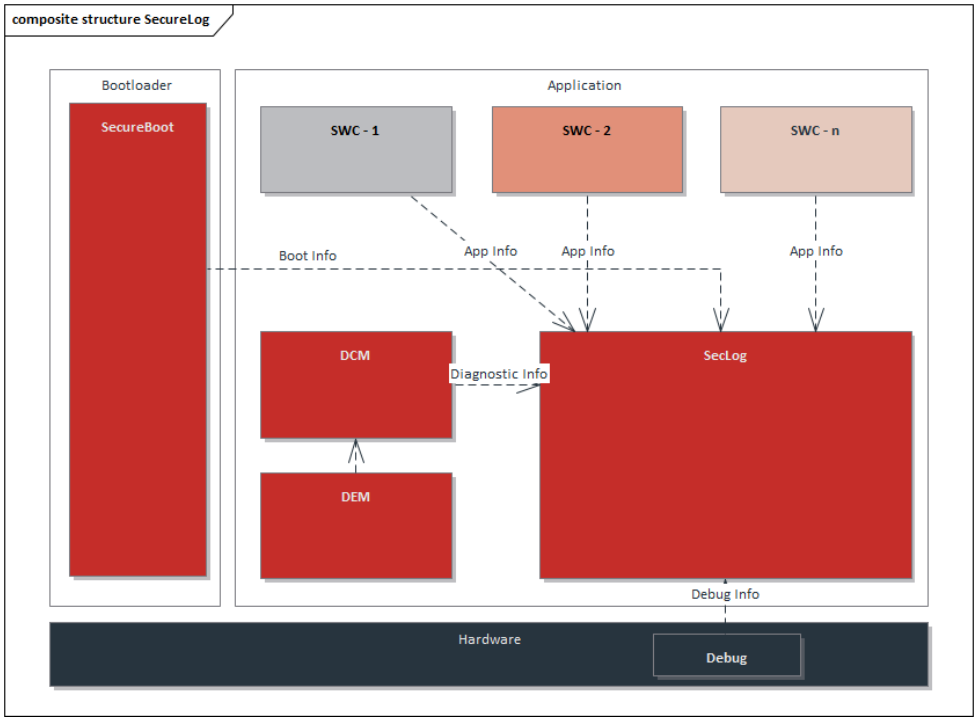


FIGURE 10 CRYPTOLIBRARY BASED ON TC2XX/TC3XX

3.3 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 information such as abnormal problems or records of authorized users generated in the process of secure communication, which can facilitate the troubleshooting of controller development as well as risk control. When the ECU generates information security vulnerabilities, the log information can be used to quickly analyze the reasons for the impact and the impact of the function, to improve the robustness of code development, and to reduce a series of impacts caused by information security vulnerabilities.



3.4 安全调试 Secure Debug

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.

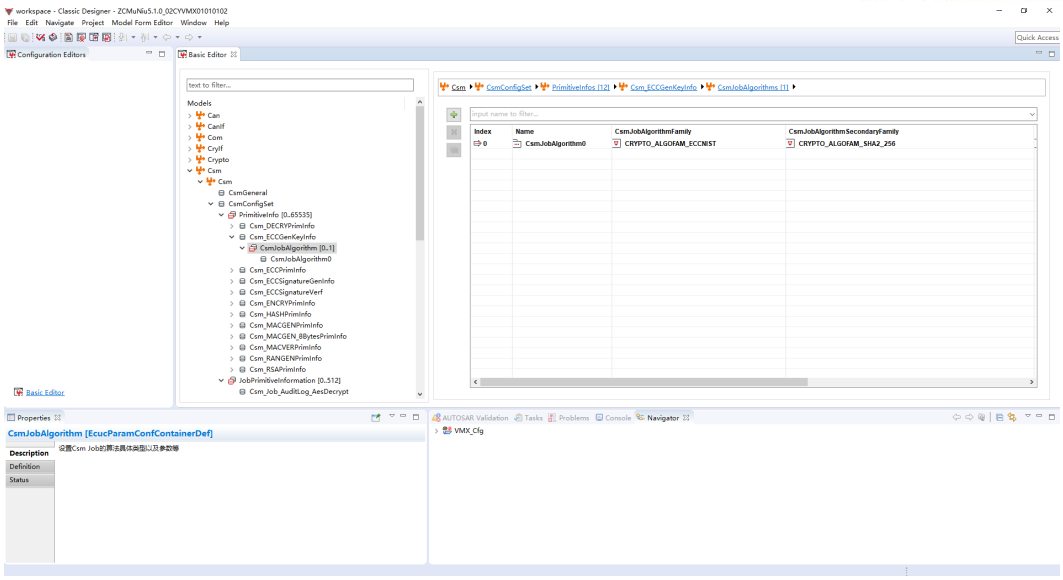
知从科技针对不同厂家芯片，制定了不同的安全调试功能方案。例如针对 NXP S32K1xx 系列芯片，可以通过安全诊断方式开启和关闭 Debug 功能，通过 Secure Diagnostic 确保授权用户可执行调试功能。

ZC has developed different secure debugging feature plans for chips from various manufacturers. For example, for NXP S32K1xx series chips, the Debug function can be enabled and disabled through secure diagnostic methods, with Secure Diagnostic ensuring that authorized users can perform debugging functions.

3.5 配置服务 Configuration Service

为了满足客户的不同项目需求，提高 CryptoLibrary 的扩展性，知从木牛配置工具实现了 CSM、CryIf、Crypto、KeyM 等模块以及加密内核的可配置性。客户可根据不同需求，在配置工具上完成 CSM、CryIf、Crypto、KeyM 等模块模块的配置工作，可生成配置代码文件，将生成的配置文件集成到工程中即可；并且可以根据需要，配置相应的 Csec 模块驱动功能，以实现接口调用。

In order to meet the different project requirements of customers and improve the scalability of CryptoLibrary, the Configuration Tool from MuNiu realises the configurability of CSM, CryIf, Crypto, KeyM and other modules as well as cryptographic kernel. Customers can complete the configuration of CSM, CryIf, Crypto, KeyM and other modules on the configuration tool according to different needs, can generate configuration code files, and the generated configuration file can be integrated into the project; and can be configured according to the needs of the corresponding Csec module driver function to achieve the interface call.



4 项目实施 PROJECT IMPLEMENTATION

编号 No.	知从 NXP 信息安全库服务输出物 ZC NXP CyberSecurity Library Service Outputs
No.1	配置集成计划 Configuration Integration Plan
No.2	需求分析报告 Requirements Analysis Report
No.3	配置工程 Configuration Project
No.4	集成工程 Integrated Project
No.5	集成手册 Integration Manual
No.6	测试报告 Test Report
No.7	发布手册 Release Manual