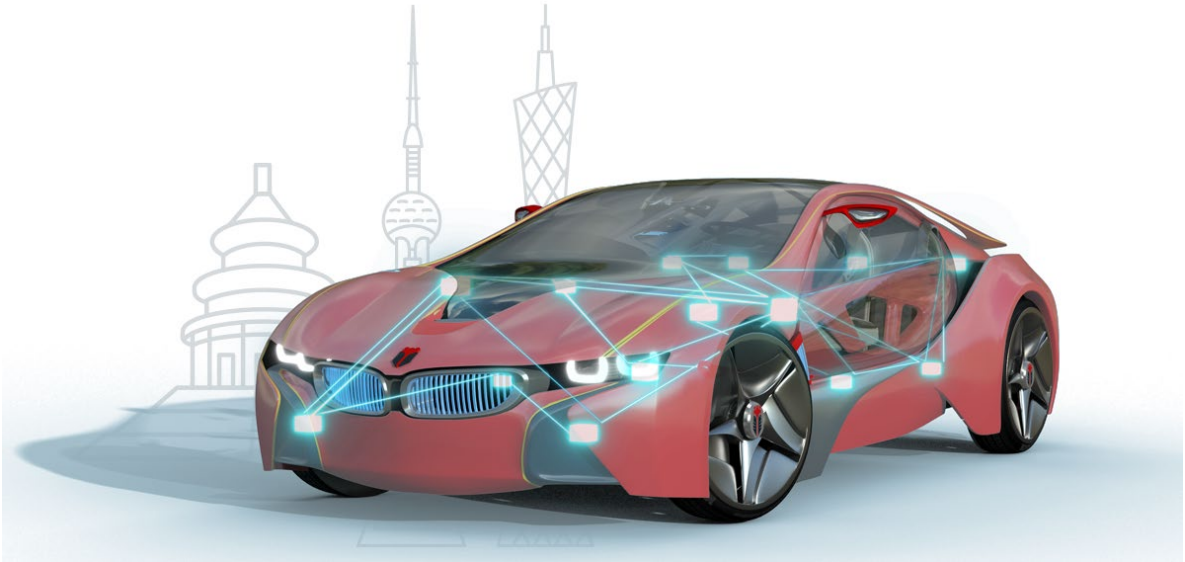
知从木牛 CRYPTOLIBRARY
瑞萨 RH850 F1KM 产品手册
ZC.MUNIU CRYPTOLIBRARY PRODUCT
MANUAL BAESD ON RENESAS RH850 F1KM

知从木牛基础软件平台信息安全库

ZC.MuNiu Basic Software Platform CryptoLibrary



知从木牛 CRYPTOLIBRARY 瑞萨 RH850 F1KM 产品手册

ZC.MUNIU CRYPTOLIBRARY PRODUCT MANUAL BAESD ON RENESAS RH850 F1KM

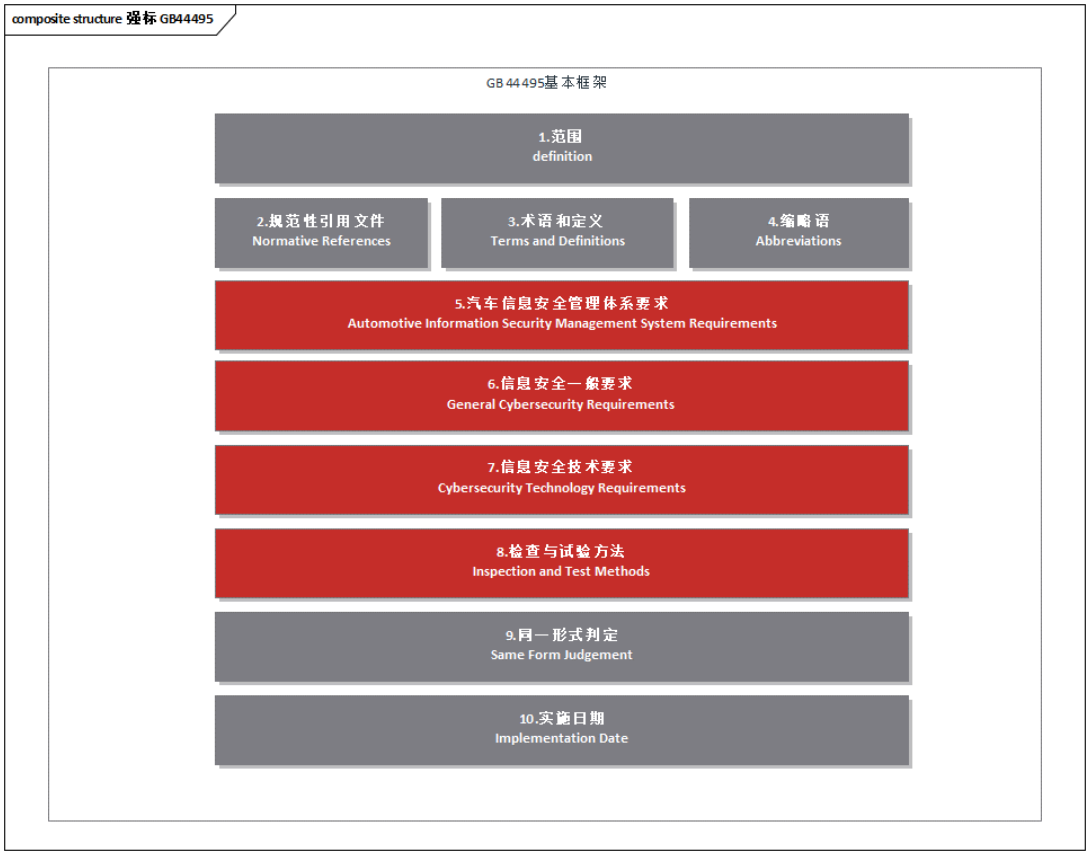
知从木牛基础软件平台信息安全库

ZC.MuNiu Basic Software Platform CryptoLibrary

1 开发背景 DEVELOPMENT BACKGROUND

随着汽车电子技术的飞速发展，车辆已经从传统的机械设备转变为高度智能化、电子化和联网的复杂系统。这些技术的引入为驾驶者带来了极大的便利，但同时也带来了新的安全挑战。汽车的电子控制系统不仅要应对功能故障的威胁，还必须防范潜在的网络攻击，因此信息安全(Cybersecurity)和功能安全(FunctionalSafety）一样,已成为现代汽车设计中不可或缺的关键要素。为应对这一挑战，国际标准化组织（ISO）于 2021 年出台了 ISO 21434 标准，专门针对道路车辆的网络安全提供指导和框架。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.



GB 44495-2024 基本框架
GB 44495-2024 BASIC FRAMEWORK

2 产品概述 PRODUCT OVERVIEW

知从科技针对瑞萨 RH850 F1KM 所开发的木牛 CryptoLibrary 包括硬件加密模块(ICUM)的内核固件(zICUM CORE)，主核的信息安全协议栈 CryptoStack（CSM、CRYIF、CRYPTO、KEYM）以及 ICUM CDD(zICUM COM、zICUM 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 ICUM 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 for the Renesas RH850 F1KM consists of the kernel firmware (zICUM CORE) for the Hardware Cryptographic Module (ICUM), the CryptoStack for the main core's Cybersecurity protocol stack (CSM, CRYIF, CRYPTO, KEYM), and the ICUM CDD (zICUM COM, zICUM 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 ICUM CDD, in addition to meeting the requirements of AUTOSAR 4.4.0 version support, can also be integrated as a separate complex driver in non-AUTOSAR environments.

知从基于 RH850 F1KM 提供的木牛 CryptoLibrary，添加了知从木牛加密协议栈（CryptoStack）包括：Csm 模块 、CryIf 模块、Crypto 模块和 KeyM 模块，使其与 RH850 F1KM 内核驱动适配。

Based on the CryptoLibrary provided by RH850 F1KM, we have added the CryptoStack, including Csm module, CryIf module, Crypto module and KeyM module, to make it compatible with the RH850 F1KM kernel driver.

- 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 module：Located in the service layer to handle user Cybersecurity 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 module：Located in the ECU abstraction layer and used to implement secure communication between the Csm module and the Crypto module
- Crypto 模块：硬件抽象层，作用为实现 Host 端与 Icum 内核间数据传输，访问相关部件，实现加解密操作
  Crypto module：Hardware abstraction layer for data transfer between Host and Icum kernel, access to related components, encryption and decryption operations.

- KeyM 模块：密钥管理与证书管理，用来实现密钥、证书与底层存储之间的交互
  KeyM module：Key management and certificate management for interaction between keys, certificates and underlying storage

简而言之，木牛 CryptoLibrary 灵活地适用于瑞萨 RH850 F1KM 产品，具有高扩展性，可以根据不同的客户项目要求进行升级配置和再开发，最终满足不同客户的信息安全需求。

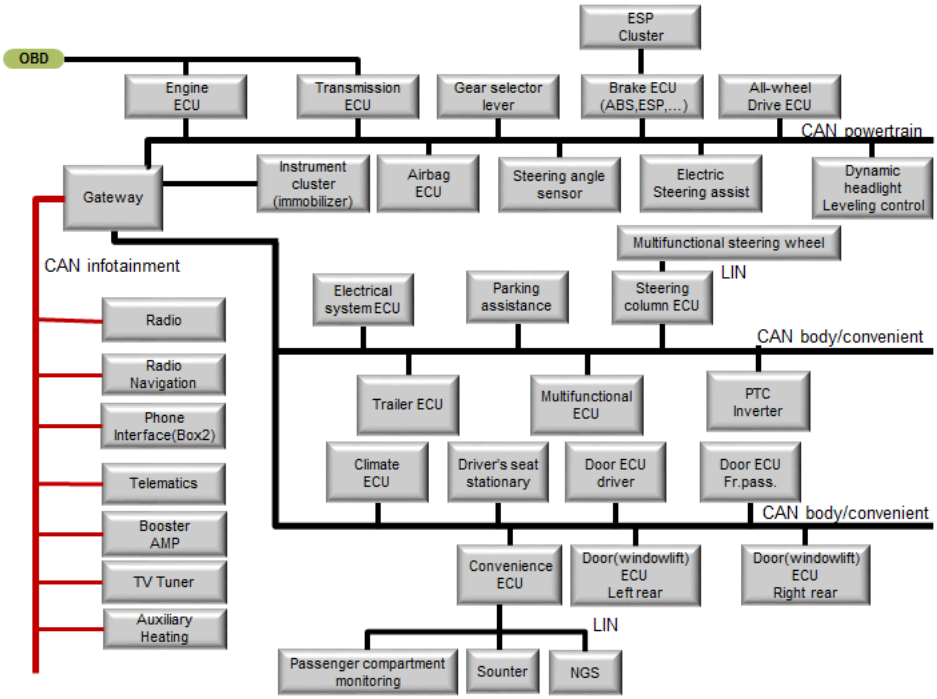
In short, the CryptoLibrary flexibly applies to Renesas RH850 F1KM products with high scalability, and can be upgraded, configured and redeveloped according to the requirements of different customer projects, ultimately meeting the Cybersecurity requirements of different customers.

3 应用领域 AREAS OF APPLICATION

木牛 CryptoLibrary 主要应用于有信息安全需求的控制器。本产品适应于汽车电子电气架构里的:

The CryptoLibrary is mainly used in controllers with Cybersecurity requirements. This product is adapted to automotive electronics in the electrical architecture:

- 电池管理系统(BMS)
  Battery Management System
- 智能驾驶控制器(ADAS)
  Advanced Driver Assistance Systems
- 电动助力转向(EPS)
  Electric Power Steering (EPS)
- 车身控制器(BCM)
  Body Control Module (BCM)
- 发动机管理系统(EMS)
  Engine Management System (EMS)



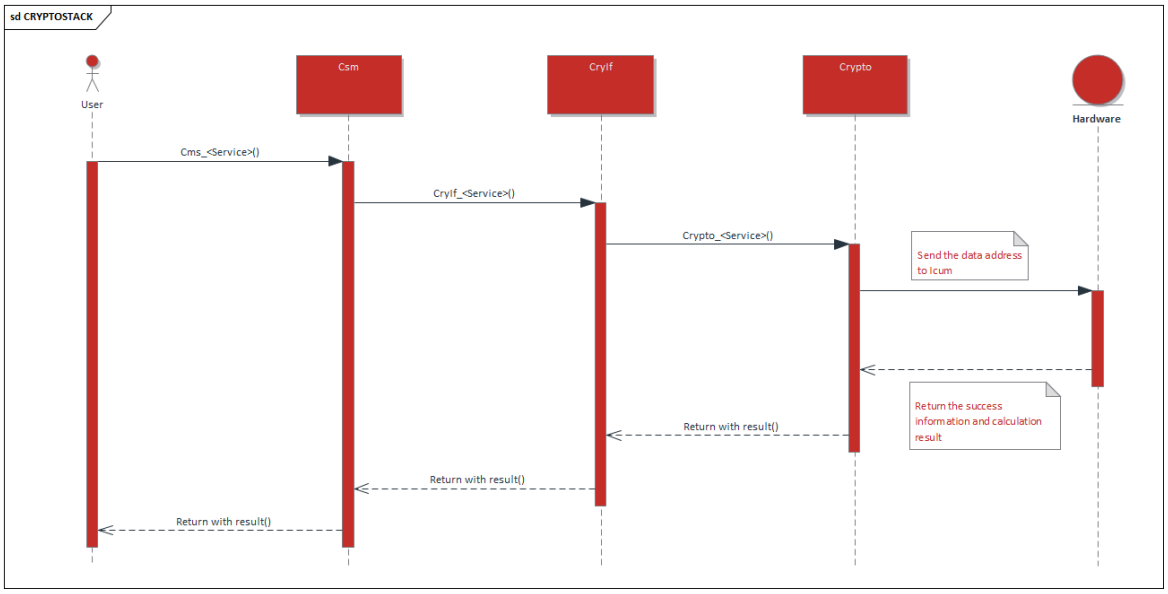
汽车电子电气架构
AUTOMOTIVE ELECTRICAL AND ELECTRONIC ARCHITECTURE

用户通过将木牛 CryptoLibrary 集成到基于 RH850 F1KM 的汽车电控单元中，可以满足 AUTOSAR 标准里所规定的汽车电控单元所具有的信息安全功能。

By integrating the CryptoLibrary into the RH850 F1KM-based automotive electronic control unit, the user can fulfil the Cybersecurity functions of the automotive electronic control unit as defined in the AUTOSAR standard.

4 功能描述 FUNCTIONAL DESCRIPTION

4.1 加密协议栈 Encryption Protocol Stack



CRYPTOSTACK 流程图
CRYPTOSTACK FLOWCHART

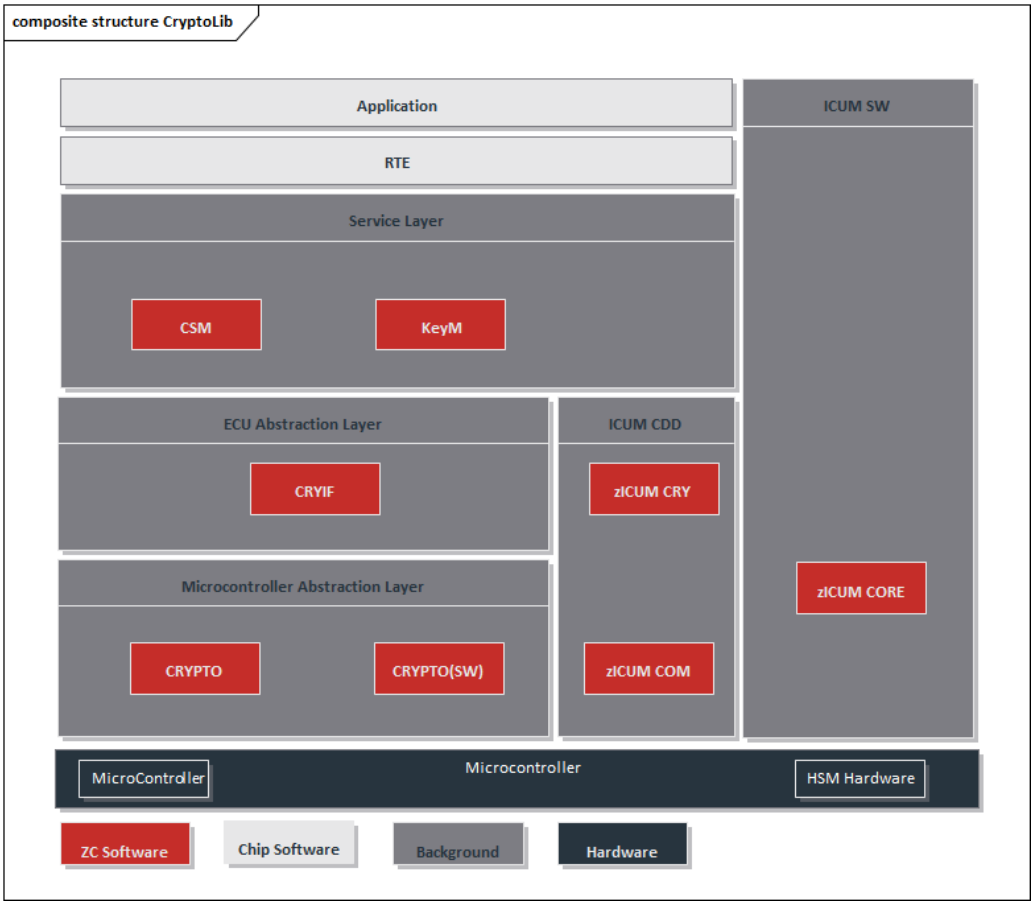
知从木牛加密协议栈主要由 Csm、CryIf、Crypto、KeyM 四个模块构成。Csm 模块通过配置 CsmJob 来实现用户所需的信息安全加密算法需求如 AES-128、CMAC、HASH、ECC、TRNG 等，并且提供接口供用户调用。CryIf 模块功能为连接服务层 Csm 模块与硬件抽象层 Crypto 模块，通过加密、解密、校验、认证等安全功能，保护数据的完整性和机密性。Crypto 模块实现 RH850 F1KM 主核与 ICMU 加密内核信息数据的传输。KeyM 模块实现密钥与证书的管理，包括对下载进 ECU 的密钥、证书解析校验，连接 ICMU 内核驱动将密钥存储进 ICMU 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 RH850 F1KM main core and the ICUM 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 ICMU kernel driver to store keys into the ICMU protected area.

4.2 木牛(MUNIU)CryptoLibrary

木牛 CryptoLibrary 的软件主要分为两部分：
The software of CryptoLibrary is divided into two main parts:

1) ICUM 硬件加密模块固件(zICUM CORE)
   ICUM hardware cryptographic module firmware (zICUM CORE)
2) RH850 G3MH 主核的 CryptoStack(CSM、CRYIF、CRYPTO、CRYPTO(SW)) 以及 ICUM CDD(zICUM COM、zICUM CRY)
   CryptoStack (CSM, CRYIF, CRYPTO, CRYPTO(SW)) for RH850 G3MH main coreand ICUM CDD(zICUM COM、zICUM CRY)



木牛 CRYPTOLIBRARY 的 AUTOSAR 集成
AUTOSAR INTEGRATION FOR CRYPTOLIBRARY

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

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

表 1 软件模块功能说明

Table 1 Software Module (TC2XX/TC3XX) Functional Description

软件模块 Software Module	模块组件 Module Component	AUTOSAR 层 AUTOSAR Layer	功能定义 Functional Definition
zICUM CORE **(加密内核)** (Encryption Core)	zICUM CORE	N/A	使用了 ICUM 内部的硬件加速器，如随机数生成器、AES-128 等（如图 4） Utilizes ICUM's internal hardware accelerators, such as random number generators, AES-128, etc. (as shown in Figure 4)
zICUM CDD **（主核）** (Main Core)	1) zICUM CRY 2) zICUM COM	CDD	微处理器 ICUM 驱动、与 ICUM 核的通信驱动、Crypto Interface 等 Microprocessor ICUM driver, communication driver with ICUM 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 的主要功能

Table 2 Main Features of MuNiu CryptoLibrary

Features		SHE standard	木牛 CryptoLibrary
AES 128 密码模式 Crypto Mode	ECB	✓	✓
	CBC	✓	✓
	CFB	✓	✓
	OFB	✓	✓
	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	✓	✓
	硬件随机数	／	✓

Features		SHE standard	木牛 CryptoLibrary
	Hardware Random		
安全启动 Secure Boot		✓	✓
非易失性密码槽 Non-Volatile Crypto Slots		10	>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	**ECC**	／	✓
	RSA	／	✓
	Ed25519(SW)	／	✓
密钥协商 Key Agreement	**ECDH(SW)**	✓	✓
	X25519(SW)	／	✓
	KDF	✓	✓
密钥存储 Key Storage	**RSA 密钥生成** RSA Key Generation	／	✓

Features		SHE standard	木牛 CryptoLibrary
	RSA 密钥存储 RSA Key Storage	／	✔
	ECC 密钥生成 ECC Key Generation	／	✔
	ECC 密钥存储 ECC Key Storage	／	✔
	Custom Externsion 支持 Custom Extension Support	／	✔
国密算法 National Cryptography Algorithms	**SM2(SW)**	／	✔
	SM3(SW)	／	✔
	SM4(SW)	／	✔

表 3 木牛 CryptoLibrary 的 SHE 功能说明

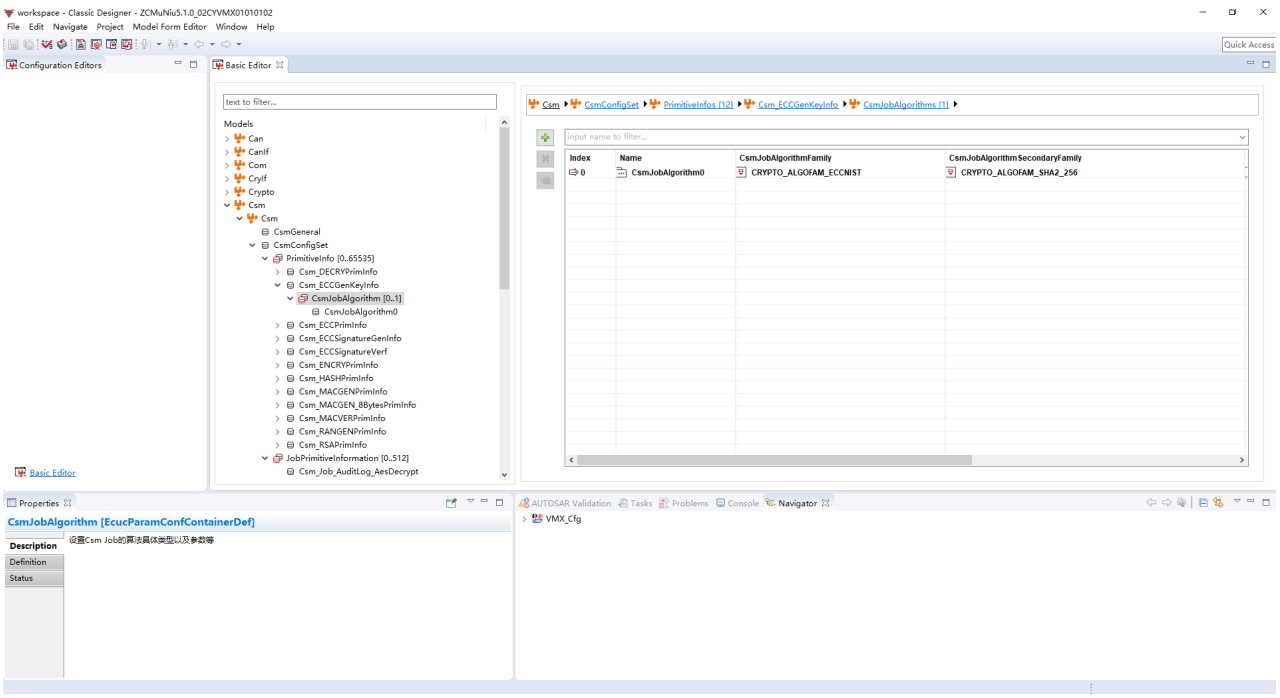
Table 3 Description of the SHE functions of the MUNIU CryptoLibrary

主要功能 key function	**解释说明** explanation
SHE 对称密钥加解密 SHE symmetric key encryption and decryption	对称式 AES-128，支持 ECB 和 CBC 加密模式对称加密 Symmetric AES-128 with support for ECB and CBC encryption modes symmetric encryption
SHE CMAC 消息认证码 SHE CMAC Message Authentication Code 生成与校验	对称式 AES-128 消息认证码 Symmetric AES-128 message authentication code

主要功能 key function	解释说明 explanation
Generation and Calibration	
SHE CMAC 安全消息认证码 SHE CMAC Security Message Authentication Code 生成与校验 Generation and Calibration	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 Supports secure CMAC validation, enabling applications to check the integrity of security-related data
SHE 明文密钥装载 SHE plaintext key loading	存储 128 位密钥到 ICUM 的 RAM, 不涉及安全协议 Stores 128-bit keys in ICUM RAM, no security protocols are involved.
SHE 密钥导出 SHE key export	对导出 RAM 密钥进行包装(加密和身份验证) Packaging of exported RAM keys (encryption and authentication)
SHE 基于安全协议的密钥装载 SHE Security protocol-based key loading	使用安全协议将 128 位密钥存储在 ICUM 非易失性存储器中 Storage of 128-bit keys in ICUM non-volatile memory using a secure protocol
SHE 随机数生成 SHE Random Number Generation	使用 AES 生成伪随机数,种子由 TRNG 生成 Generate pseudo-random numbers using AES, seeded by TRNG
SHE 安全启动 SHE Secure Start	验证应用程序启动代码的 CMAC. Verify the CMAC of the application startup code.
SHE 调试模式 SHE Debug Mode	使用安全协议启用对 ICUM 调试接口的访问 Enabling access to the ICUM debug interface using security protocols
SHE 状态获取 SHE Status Acquisition	获取 SHE 状态. Get SHE status
SHE 命令取消 SHE command cancellation	取消当前正在执行的操作. Cancels the current operation.

主要功能 key function	解释说明 explanation
SHE 错误报告 **SHE Error Reporting**	除了 CSM 返回代码之外，还可以通过 AUTOSAR 机制报告 SHE 错误 In addition to the CSM return code, SHE errors can be reported through the AUTOSAR mechanism
SHE 超时处理 **SHE Timeout Handling**	如果 ICUM 响应时间超过预定义的限制，则报告错误 If the ICUM response time exceeds a predefined limit, an error is reported
应用软件更新支持 (Cipher 和 MAC) **Application Software Update Support (Cipher and MAC)**	在应用软件的更新过程中也可以使用密码和 MAC 功能 Password and MAC functions can also be used during application updates
硬件随机数 **hardware random number**	支持生成真随机数 Support for generating true random numbers
AES 加密扩展 (OFB, CFB, CTR, XTS,GCM) **AES encryption extensions (OFB, CFB, CTR, XTS,GCM)**	支持额外的 AES 模式 Supports additional AES modes
密钥扩展 **key expansion**	支持扩展更多的非易失性密钥 Support for extending more non-volatile keys

4.3 配置工具 Configuration tools



知从木牛 CRYPTOSTACK 配置界面图
ZC.MUNIU CRYPTOSTACK CONFIGURATION DIAGRAM

为了满足客户的不同项目需求，提高木牛 CryptoLibrary 的扩展性，瑞萨 RH850 F1KM 实现了各个模块可配置性，并且实现了木牛 CryptoLibrary 的配置工具。客户可根据不同需求，在配置工具上完成 Safety Library 各个模块的配置工作，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。

In order to meet the different project requirements of customers and improve the scalability of the CryptoLibrary, Renesas RH850 F1KM realises the configurability of each module and implements the configuration tool for the CryptoLibrary. Customers can complete the configuration work of each module of Safety Library on the configuration tool according to different requirements, and can generate configuration code files and integrate the generated configuration files into the project.

4.4 应用场景 Application scenarios

■ 安全启动 Secure Boot

- 基于硬件加密方案
  Hardware-based encryption programme
- 基于软件加密方案
  Software-based encryption programme
- 密钥存储管理方案
  keystore management programme
- 安全启动失效分析
  Safe Start Failure Analysis
- 产线生产模式方案
  Line Production Model

■ 安全升级 Security Upgrade

- X.509 证书授权管理
  X.509 Certificate Authority Management
- A/B 区备份升级
  A/B Zone Backup Upgrade
- APP 数据压缩下载
  APP Data Compression Download
- APP 数据安全升级
  APP Data Security Upgrade
- 配套上位机工具(玄武上位机工具)
  Supporting Upper Unit Tool (Genbu Upper Unit Tool)
- 支持不同 OEM 厂家规范
  Supports different OEM

■ 安全日志 Security log

- 安全事件日志签名存储
  Security Event Log Signature Storage

■ 安全诊断 Safety Diagnostics

- 证书存储解析功能
  Certificate store parsing function
- 公私钥存储解析功能
  Public-Private Key Storage Resolution Function
- 密钥更新管理功能
  key update management function
- 支持 UDS0x29 服务
  Support for UDS0x29 services
- 支持 UDS0x84 服务
  Support for UDS0x84 services
- 支持集成信息安全库
  Support for integrated information security libraries

■ 安全存储 Secure Storage

- 对称/非对称密钥安全存储
  Symmetric/asymmetric key secure storage
- X.509 证书安全存储
  X.509 certificate secure storage
- MAC 值存储
  MAC value storage

■ 安全调试 Secure Commissioning

- 下线调试加密流程
  offline debugging encryption process
- 诊断解密调试权限
  Diagnostic Decryption Debugging Privileges
- 诊断获取密钥信息
  Diagnostics Get Key Information

配置环境	Configuring the Environment
Hardware (Chip)	RH850 F1KM
Compilers Supported	Green Hills MULTI v7.1.6
Evaluation Hardware	RH850 F1KM R7F7015843AFP
Debugger	Lauterbach (TRACE32 2023/02) Isystem (IC5700)
Configuration Tools	Muniu_v5.0.5
Configuration Environment	Win10 64bit

Green Hills 编译器选项	Green Hills Compiler Options
Green Hills 编译选项 **Green Hills Compilation Options**	-mcpu=RH850-F1KM -c –Os -ggdb3 -mcpu= RH850-F1KM -mthumb -mlittle-endian -fomit-frame-pointer -msoft-float -fno-common -Wall -Wextra -Wstrict-prototypes -Wno-sign-compare -fstack-usage -fdump-ipa-all -std=c99
Green Hills 链接选项 **Green Hills Link Options**	-mcpu= RH850-F1KM -msoft-float -mthumb -e _start -nostartfiles -static -lc -lm -lgcc -lnosys

6 证书 CERTIFICATES

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 一 月二十五 日

木牛软件产品登记证书
MUNIU SOFTWARE PRODUCT REGISTRATION CERTIFICATE