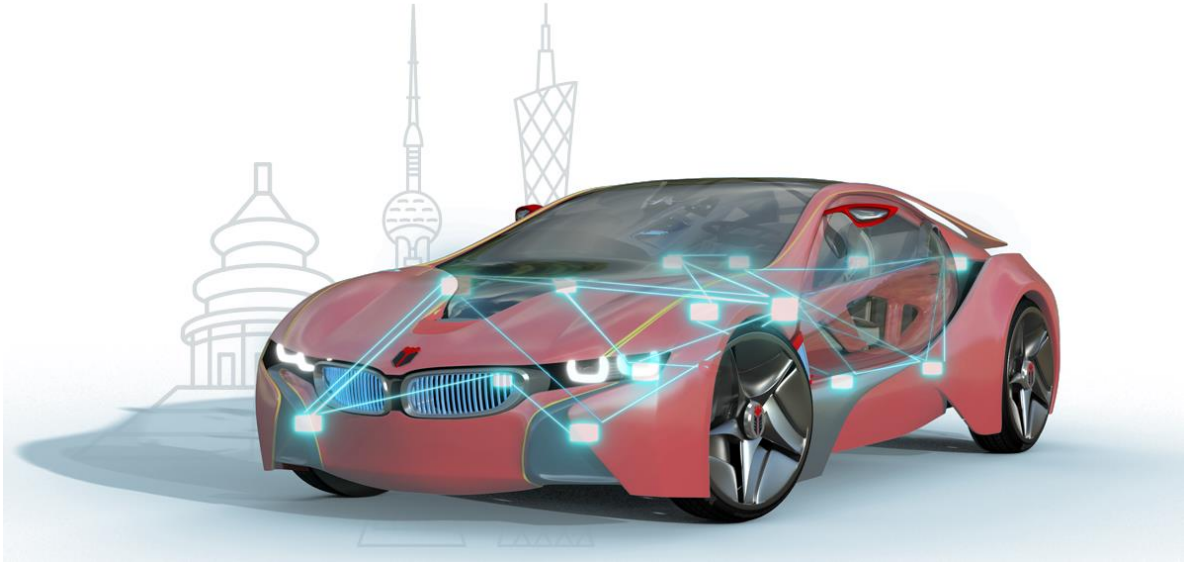
知从木牛 CRYPTOLIBRARY 英飞凌 TRAVEOT2G 产品手册

ZC.MUNIU CYBERSECURITY LIBRARY PRODUCT MANUAL BASED ON INFINEON TRAVEOT2G

知从木牛基础软件平台信息安全库

ZC.MuNiu Basic Software Platform Cybersecurity Library



知从木牛 CRYPTOLIBRARY 英飞凌 TRAVEOT2G 产品手册
ZC.MUNIU CYBERSECURITY LIBRARY PRODUCT MANUAL BASED ON INFINEON TRAVEOT2G

知从木牛基础软件平台信息安全库

ZC MuNiu Basic Software Platform Cybersecurity Library

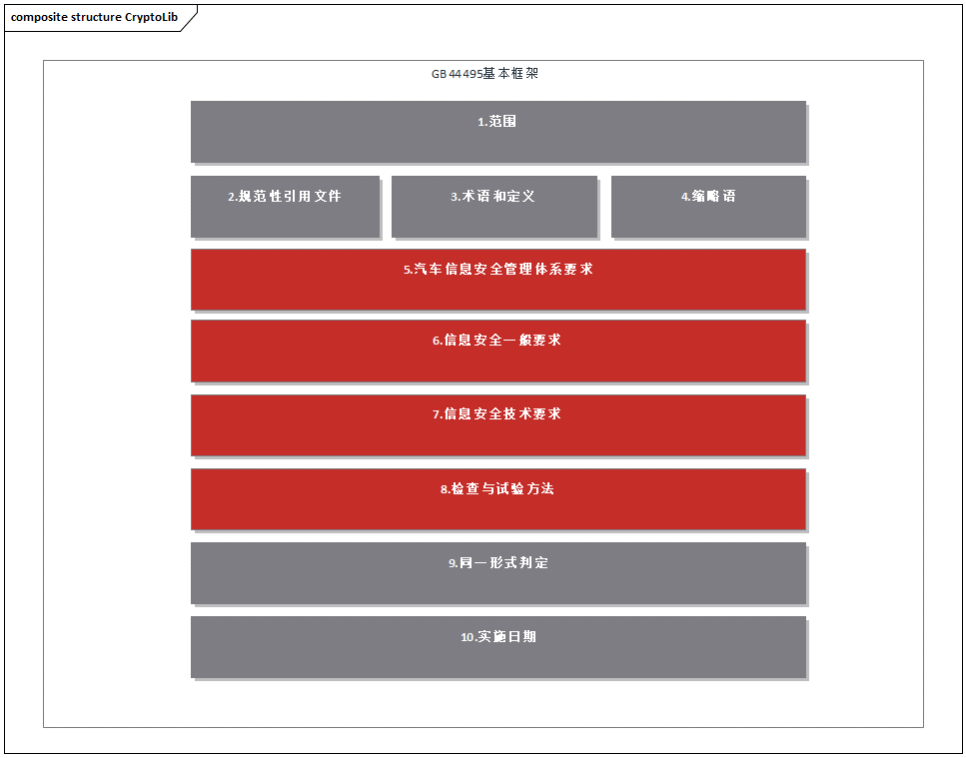
1 开发背景 DEVELOPMENT BACKGROUND

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。

With the rapid development of automotive electronics technology, vehicles have transformed from traditional mechanical devices into highly intelligent, electronic, and network - connected complex systems. The introduction of these technologies has brought great convenience to drivers, but at the same time, it has also presented new security challenges. The electronic control systems of vehicles not only need to deal with the threat of functional failures but also must guard against potential cyber - attacks. Therefore, just like Functional Safety, Cybersecurity has become an essential key element in modern vehicle design.

To address this challenge, the International Organization for Standardization (ISO) introduced the ISO 21434 standard in 2021, which specifically provides guidance and a framework for the cybersecurity of road vehicles. With the official launch of the "Technical Requirements for Vehicle - level Cybersecurity" standard in China in the second half of 2024, the technical specifications and implementation standards in the field of automotive cybersecurity have been further refined, marking the entry of the automotive safety field into an era of truly strict supervision.



GB 44495-2024 基本框架

GB 44495 - 2024 BASIC FRAMEWORK

2 产品概述 PRODUCT OVERVIEW

知从科技针对英飞凌 TRAVEO T2G 所开发的木牛 CryptoLibrary 包括加密模块(HSM)的固件(zHSM CORE)，主核的加密协议栈 CryptoStack（CSM、CRYIF、CRYPTO、KEYM）以及 HSM CDD(zHSM COM、zHSM CRY)。木牛 CryptoLibrary 除了满足 NIST 主流国际密码算法，如 AES、HASH、TDES、ECC 和 TRNG/PRNG 等，并且基于知从软件算法库扩展了多种其他算法，包括国密算法 SM2/3/4、Curve25519/X25519 等，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 MuNiu CryptoLibrary developed by ZC for Infineon TRAVEO T2G encompasses the firmware of the encryption module (HSM) (zHSM CORE), the encryption protocol stack CryptoStack (CSM, CRYIF, CRYPTO, KEYM) for the main core, along with HSM CDD (zHSM COM, zHSM CRY).

The MuNiu CryptoLibrary not only complies with mainstream international cryptographic algorithms of NIST, such as AES, HASH, TDES, ECC, and TRNG/PRNG. Based on ZC's software algorithm library, it has extended a variety of other algorithms, including national cryptographic algorithms like SM2/3/4, Curve25519/X25519, etc. Additionally, it can expand multiple functions based on these algorithms, such as symmetric encryption and decryption, asymmetric signature generation and verification, secure boot, secure flashing, and SecOC.

Besides meeting the version requirements of AUTOSAR 4.4.0, CryptoStack and HSM CDD can also be integrated as a single complex driver in non - AUTOSAR environments.

知从基于 TRAVEO T2G 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 T2G HSM 加密模块驱动适配。

Based on the TRAVEO T2G, ZC provides the MuNiu CryptoLibrary and has added the ZC MuNiu encryption protocol stack (CryptoStack), which includes the Csm module, CryIf module, Crypto module, and KeyM module, enabling it to be adapted to the T2G HSM encryption module 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, it is used to handle the configuration management and scheduling of user information security tasks.
- 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: Situated in the ECU abstraction layer, its function is to achieve 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 HSM 模块间数据传输，访问相关部件，实现加解密操作
- Crypto module: Hardware abstraction layer, used to implement data transmission between the Host end and HSM module, access related components, and perform 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, used to achieve interaction between keys, certificates, and underlying storage

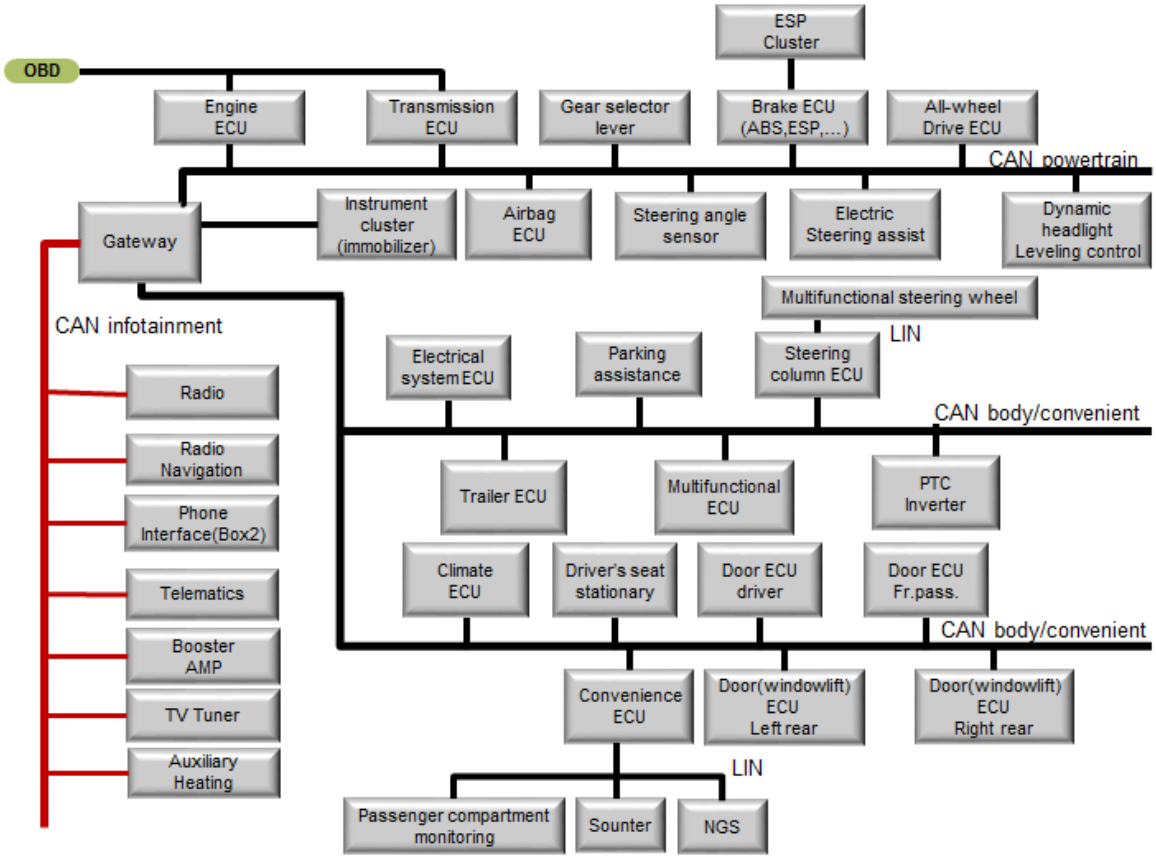
简而言之，木牛 CryptoLibrary 灵活地适用于英飞凌 TRAVEO T2G 产品，具有高扩展性，可以根据不同的客户项目要求进行升级配置和再开发，最终满足不同客户的信息安全需求。

In short, the MuNiu CryptoLibrary is flexibly applicable to Infineon TRAVEO T2G products. It features high scalability, allowing for upgrade configuration and redevelopment according to the requirements of different customer projects, ultimately meeting the diverse information security needs of various customers.

3 应用领域 APPLICATION FIELDS

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： 动力域控制器， 车身域控制器， 安全域控制器和信息域控制器。

The MuNiu CryptoLibrary is mainly applied to controllers with information security requirements. This product is suitable for use in the automotive electronic and electrical architecture, including power domain controllers, body domain controllers, safety domain controllers, and infotainment domain controllers.



汽车电子电气架构

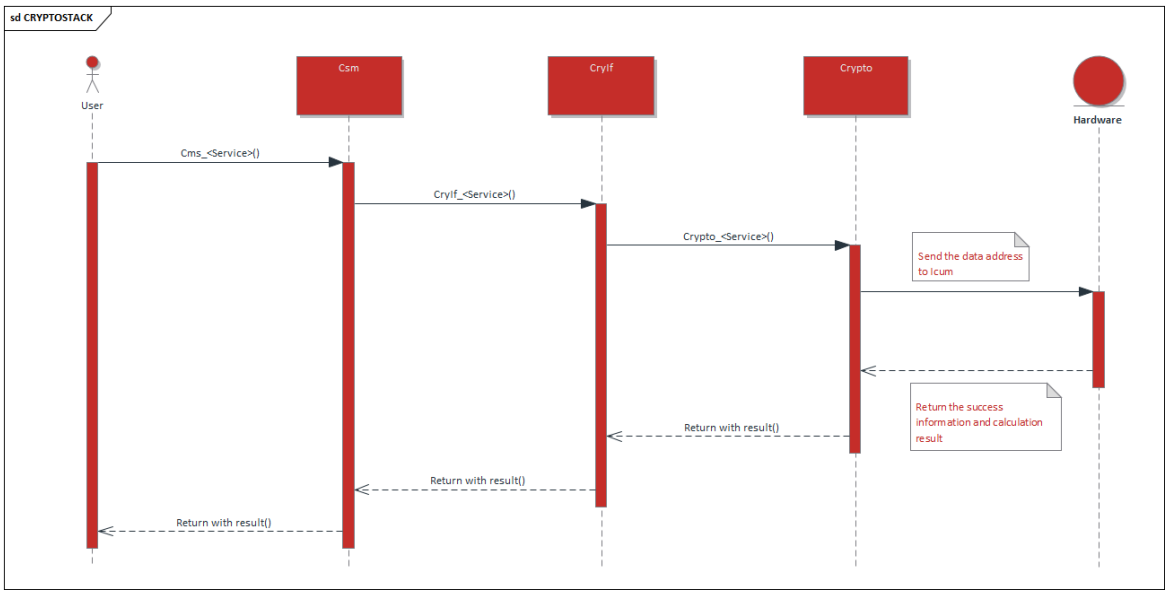
AUTOMOTIVE ELECTRONIC AND ELECTRICAL ARCHITECTURE

用户通过将木牛 CryptoLibrary 集成到基于 TRAVEO T2G 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 MuNiu CryptoLibrary into the TRAVEO T2G - based automotive electronic control units (ECUs), users can meet the information security functions required for automotive ECUs as specified in the AUTOSAR standard.

4 功能描述 FUNCTIONAL DESCRIPTION

4.1 加密协议栈 Crypto Stack



CRYPTOSTACK 流程图

FLOWCHART OF CRYPTOSTACK

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 TRAVEOT2G 主核与 HSM 模块信息数据的传输。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 模块驱动将密钥存储进 HSM 受保护区域等功能。

The ZC.MuNiu encryption protocol stack is mainly composed of four modules: Csm, CryIf, Crypto, and KeyM. The Csm module meets users' requirements for encryption algorithms of information - security software or hardware, such as AES - 128, CMAC, HASH, TRNG, etc., by configuring CsmJob, and provides interfaces for users to call.

The CryIf module serves to connect the Csm module in the service layer with the Crypto module in the hardware abstraction layer. It safeguards data integrity and confidentiality through security functions like encryption, decryption, verification, and authentication.

The Crypto module enables the transmission of information and data between the main core of TRAVEO T2G and the HSM module.

The KeyM module manages keys and certificates. Its functions include parsing and verifying the keys and certificates downloaded into the ECU, and connecting to the HSM module driver to store the keys in the protected area of HSM.

4.2 木牛 CryptoLibrary MuNiu CryptoLibrary of ZC

4.2.1 静态架构设计 Static Architecture Design

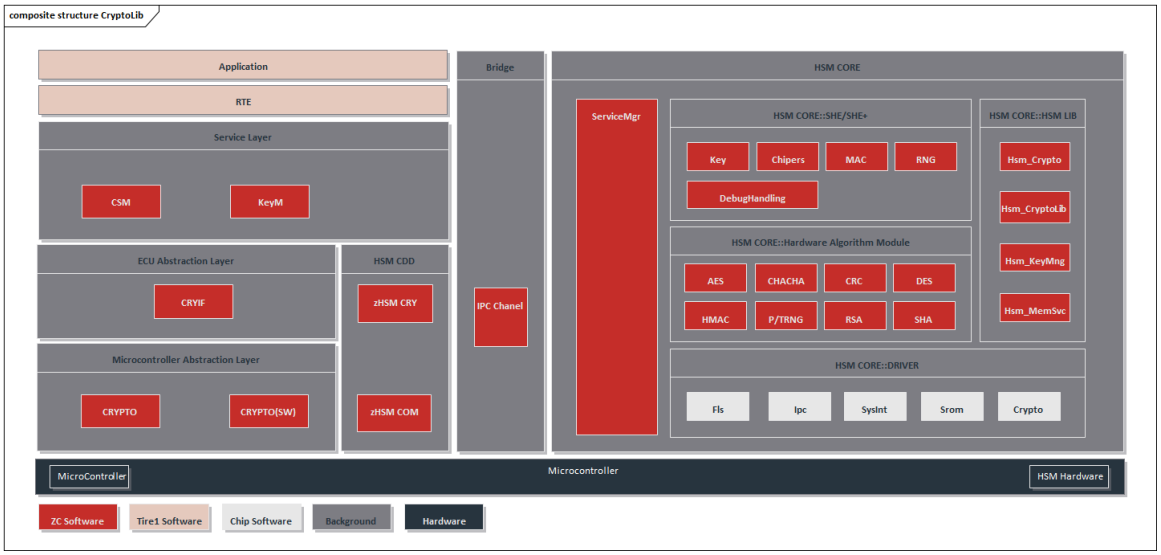


图 4.1 CYT4BB 信息安全库软件静态架构

FIGURE 4.1 STATIC ARCHITECTURE OF CYT4BB CYBERSECURITY LIBRARY SOFTWARE

4.2.2 架构描述 Architecture Description

CYT4BB 信息安全库软件架构主要包含 2 部分： CM7 核 Service 层调用接口，CM0 核各模块驱动，其中：

- CM7 核 Service 层调用接口

  CM7 核不含 CryptoStack，只包含 HSM CDD 部分，其中 zHSM CRY 包含：AES、CHACHA、CMAC、CRC、DEBUGHANDLING、DES、TDES、ED25519、GETUID、HMAC_SHA1/SHA2/SHA3、KDF、KEYLOAD、PRNG/TRNG、RSA、SHA 等模块调用接口。zHSM COM 为核间通信相关传输接口。
- CM0 核各模块驱动

  CM0 核包含各模块驱动，其中 SHE/SHE+模块包含 AUTOSAR_ScureHardwareExtension 文档相关要求模块，包括 SHE Key、Chipers、MAC、RNG 等模块。硬件加速模块如上图所示。HSM LIB 为知从 HSM 软件算法库的集成，其中包含：Ed25519、GETUID、KDF 等用软件算法实现的模块

  The CYT4BB information security library software architecture mainly consists of two parts: the CM7 core service layer call interface, and the CM0 core module drivers. Among them:

- CM7 Core Service Layer Call Interface

  The CM7 core does not contain CryptoStack, only the HSM CDD part, where zHSM CRY includes: AES、CHACHA、CMAC、CRC、DEBUGHANDLING、DES、TDES、ED25519、GETUID、HMAC_SHA1/SHA2/SHA3、KDF、KEYLOAD、PRNG/TRNG、RSA、SHA Wait for the module to call the interface. ZHSM COM is a transmission interface related to inter core communication.

- CM0 core module drivers

  The CM0 core contains various module drivers, among which the SHE/SHE+module includes AUTOSAR_ScureHardwareExtension document related requirement modules, including SHE Key, Chipers, MAC, RNG and other modules. The hardware acceleration module is shown in the above figure. HSM LIB is an integration of the HSM software algorithm library, which includes modules such as Ed25519, GETUID, KDF implemented using software algorithms

4.2.3 启动及运行阶段流程 Start up and operation phase process

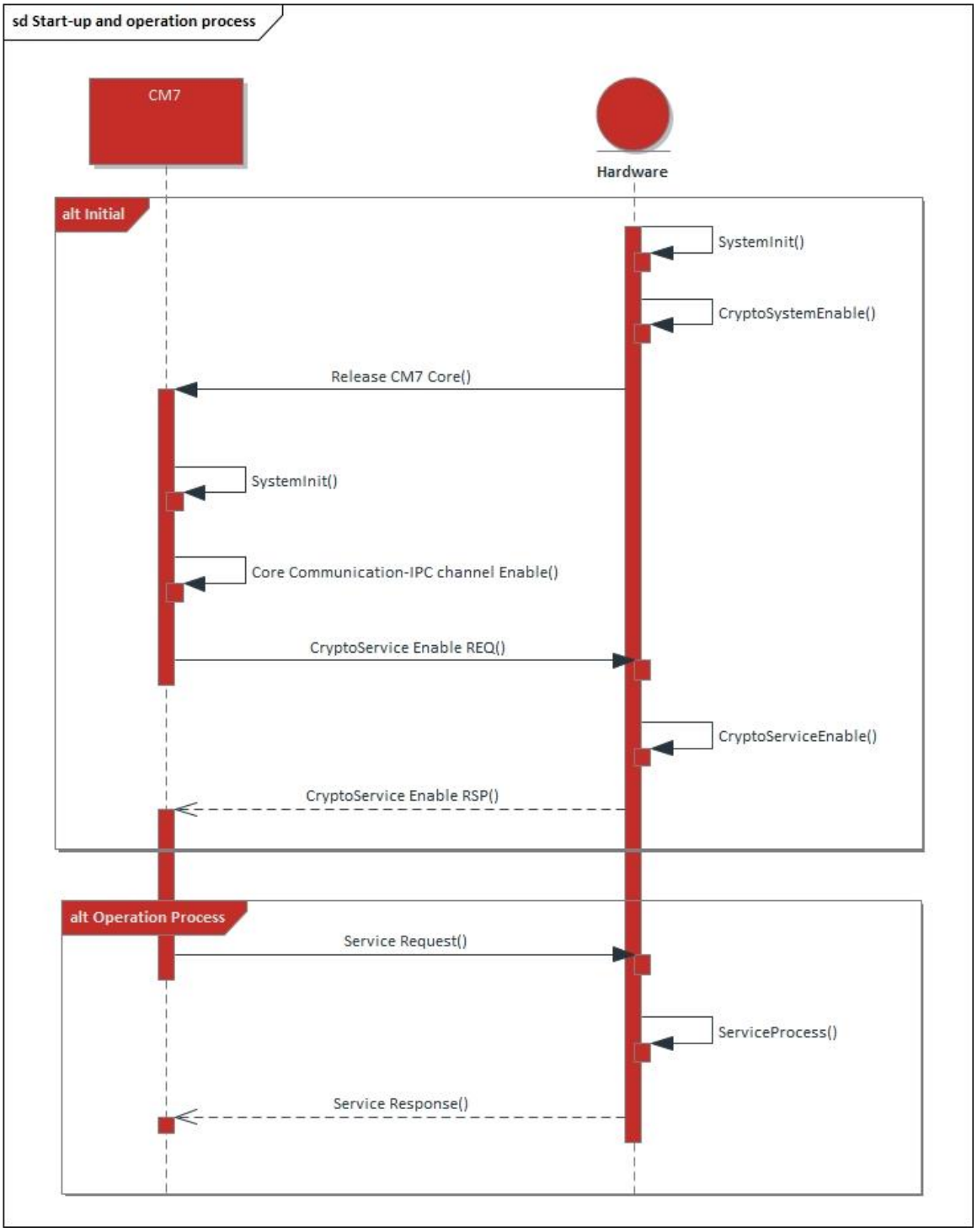


图 4.2 CYT4BB 信息安全库软件上电启动流程

FIGURE 4.2 STARTUP PROCESS OF CYT4BB CYBERSECURITY LIBRARY SOFTWARE

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 contains two sub - modules: the zHSM CRY module which is the call interface of the Crypto layer, and the zHSM COM module for HSM communication. The functional descriptions of each module are shown in Table 1.

表 1 软件模块功能说明

Table 1 Functional Description of Software Modules

软件模块 Software Module	模块组件 Module Components	AUTOSAR Layer	功能定义 Functional Definition
zHSM CORE (加密内核) (Encryption Kernel)	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） It utilizes the internal hardware accelerators of HSM, such as the random number generator, 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 the 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 information security key and JOB management, which are used for configuration 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。

The MuNiu CryptoLibrary also supports the SHE standard. Compared with the standard SHE, the CryptoLibrary has some functional expansions, including support for software or hardware algorithms. The main functions and differences are shown in Tables 2 and 3.

表 2 木牛 CryptoLibrary 的主要功能

Table 2 Main Functions of ZC.MuNiu CryptoLibrary

Features		SHE standard	木牛 CryptoLibrary MuNiu CryptoLibrary
AES 128 密码模式 AES 128 Cipher Modes	ECB	✓	✓
	CBC	✓	✓
	CFB	✓	✓
	OFB	✓	✓
	XTS	✓	✓
消息认证码 Message Authentication Code	AES128-CMAC	✓	✓
	GMAC	／	✓
	HMAC	／	✓
	SM3-HMAC	／	✓
	SM4-CMAC	／	✓
随机数生成器 Random Number Generator	伪随机数 Pseudorandom number	✓	✓

	真随机数 True Random Number	✓	✓
	硬件随机数 Hardware random number	/	✓
安全启动 Secure Boot		✓	✓
非易失性密码槽 Non - Volatile Cryptographic Slot		10	>50
可易失性密码槽 Volatile Cryptographic Slot		✓	✓
支持可用于 UDS0x29 认证密钥 Support authentication keys that can be used for UDS0x29.		/	✓
安全诊断 UDS 0x29 认证 Security diagnostic UDS 0x29 authentication		/	✓
非对称加密 Asymmetric Encryption	RSA-OAEP 2048	/	✓
	RSA-OAEP 3072	/	✓
	RSA-OAEP 4096	/	✓
	RSA-PKCS 2048	/	✓
	RSA-PKCS 3072	/	✓
	RSA-PKCS 4096	/	✓

	ECDSA-SECP256r1	/	✓
	ED25519	/	✓
	ECDSA-SM2	/	✓
对称加密 symmetric encryption	3DES	/	✓
	AES-GCM	/	✓
	SM4-ECB	/	✓
	SM4-CBC	/	✓
	AES-128	/	✓
	AES-192	/	✓
	AES-256	/	✓
哈希算法 Hash algorithm	SHA2-256	/	✓
	SHA2-512	/	✓
	SHA3-256	/	✓
	SHA3-512	/	✓
	SHA-1(SHA-160)	/	✓

	MD5	/	✓
密钥协商 Key Negotiation	ECDH	/	✓
	ED25519	/	✓
	KDF	✓	✓
	DH	/	✓
	ECDH-SM2	/	✓
	RSA	/	✓
密钥存储 Key Storage	RSA 密钥生成 RSA Key Generation	/	✓
	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 Cryptographic Algorithm	SM2	/	✓
	SM3	/	✓

	SM4-ECB	／	✓
	SM4-CBC	／	✓

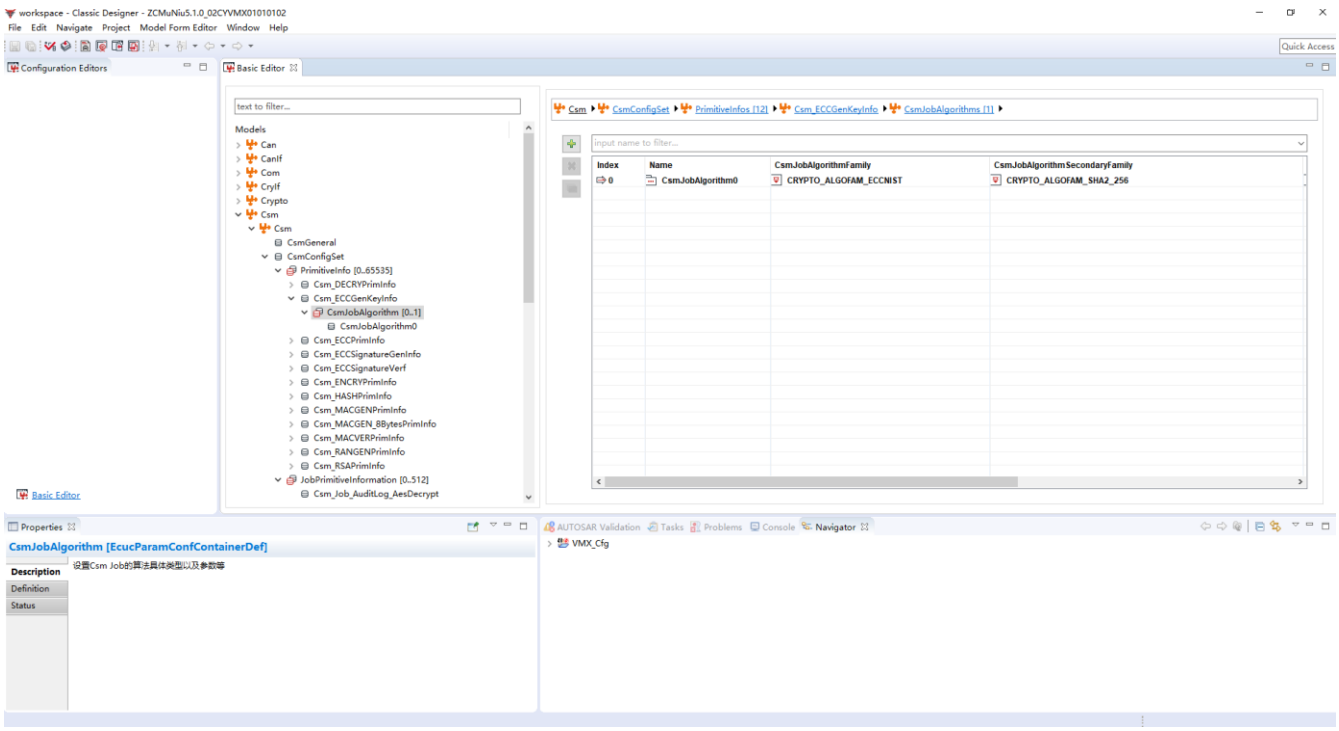
表 3 木牛 CryptoLibrary 的 SHE 功能说明

Table 3. Mu Niu CryptoLibrary's SHE Function Description

主要功能 Main Functions	解释说明 Explanation and Illustration
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, supporting symmetric encryption in ECB and CBC encryption modes
SHE CMAC 消息认证码 生成与校验 SHE CMAC Message Authentication Code Generation and Verification	对称式 AES-128 消息认证码 Symmetric AES - 128 Message Authentication Code
SHE CMAC 安全消息认证码 生成与校验 Generation and Verification of SHE CMAC Secure Message Authentication Code	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 verification, 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 HSM 的 RAM, 不涉及安全协议 Store a 128 - bit key into the RAM of HSM without involving security protocols.
SHE 密钥导出 SHE Key Derivation	对导出 RAM 密钥进行包装(加密和身份验证) Wrap (encrypt and authenticate) the key exported from the RAM.
SHE 基于安全协议的密钥装载 SHE Key Loading	使用安全协议将 128 位密钥存储在 HSM 非易失性存储器中 Store the 128 - bit key in the non - volatile memory of HSM using a security protocol.

Based on Security 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, with the seed generated by TRNG.
SHE 安全启动 SHE Secure Boot	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 HSM 调试接口的访问 Enable access to the HSM debug interface using a security protocol.
SHE 状态获取 SHE Status Retrieval	获取 SHE 状态. Obtain the SHE status.
SHE 命令取消 SHE Command Cancellation	取消当前正在执行的操作. Cancel the currently executing operation.
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 Besides the CSM return code, SHE errors can also be reported through the AUTOSAR mechanism.
SHE 超时处理 SHE Timeout Handling	如果 HSM 响应时间超过预定义的限制，则报告错误 If the HSM response time exceeds the predefined limit, an error is reported.
应软件更新支持 Software update support should be provided (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 HSM and MAC functions can also be used during the update process of the application software.
硬件随机数 Hardware Random Numbers	支持生成真随机数 Supports the generation of true random numbers.
AES 加密扩展 AES Encryption Modes (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 Supports the expansion of more non - volatile keys.

4.3 配置工具 Configuration Tools



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

为了满足客户的不同项目需求，提高木牛 CryptoLibrary 的扩展性，英飞凌 TRAVEO T2G 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。

To meet the diverse project requirements of customers and enhance the scalability of the MuNiu CryptoLibrary, Infineon TRAVEO T2G has implemented the configurability of each module and developed a configuration tool for the MuNiu CryptoLibrary. Customers can, according to their different needs, complete the configuration of each module of the Safety Library on the configuration tool. The tool can generate configuration code files, which can then be integrated into the project.

5 配置环境 CONFIGURATION ENVIRONMENT

配置环境 CONFIGURATION ENVIRONMENT	
Hardware (Chip)	TRAVEO T2G
Compilers Supported	IAR EW for Arm 9.30.1
Evaluation Hardware	R7F702300 EABA-C
Debugger	Lauterbach (TRACE32 2023/02) Isystem (IC5700)
Configuration Tools	Muniu_v5.0.5
Configuration Environment	Win10 64bit

IAR EW for Arm 9.30.1 编译器选项 IAR EW for Arm 9.30.1 Compiler Options	
IAR EW for Arm 9.30.1 编译选项 **IAR EW for Arm 9.30.1 Compilation Options**	-G -dual_debug # Generation of DWARF debugging information in the object file (in addition to the GHS .dbo format) for use with 3rd party debuggers -C99 -align4 --short_enum --no_commons --no_alternative_tokens -asm3g -preprocess_assembly_files --preprocess_linker_directive_full -nostartfiles -globalcheck=normal -globalcheck_qualifiers --prototype_errors -Wformat -Wimplicit-int -Wshadow

	-Wtrigraphs -Wundef -reject_duplicates -object_dir=objs :sourceDir=. --no_wrap_diagnostics
IAR EW for Arm 9.30.1 链接选项 **IAR EW for Arm 9.30.1 Linking Options**	--preprocess_linker_directive_full

6 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
CERTIFICATE OF REGISTRATION OF MUNIU SOFTWARE COPYRIGHT

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

重点实验室

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