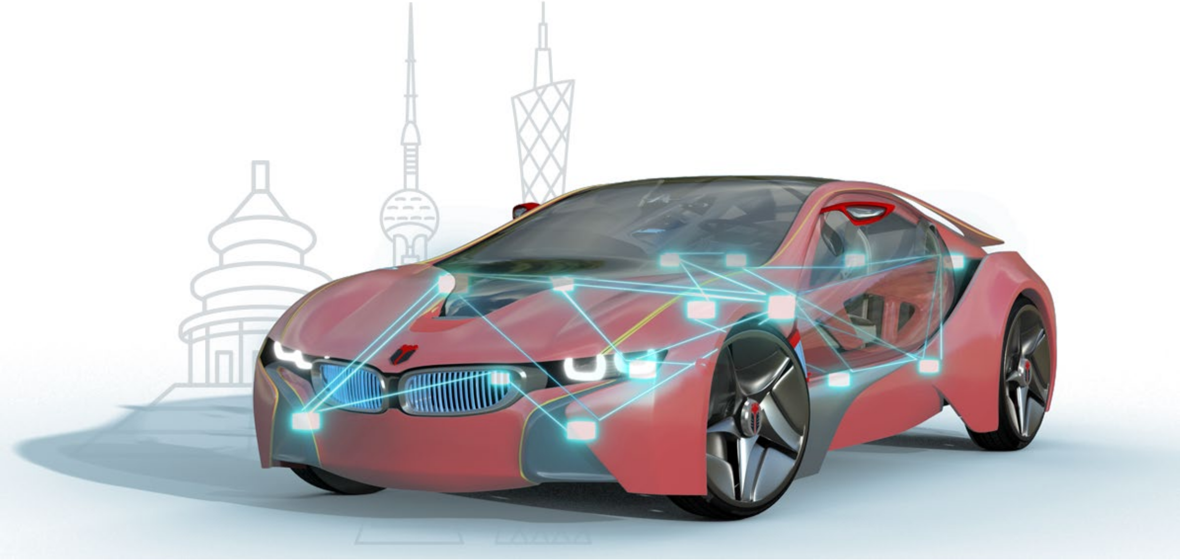
知从木牛 CryptoLibrary 英飞凌 TC3XX 产品手册

ZC.MuNiu CryptoLibrary Product Manual Based On Infineon TC3XX

知从木牛基础软件平台

ZC.MuNiu Basic Software Platform



知从木牛 CryptoLibrary 英飞凌 TC3XX 产品手册

ZC.MUNIU CRYPTOLIBRARY PRODUCT MANUAL BASED ON INFINEON TC3XX

知从木牛基础软件平台

ZC.MuNiu Basic Software Platform

1 开发背景 DEVELOPMENT BACKGROUND

智能网联汽车在全球范围内蓬勃发展，由此带来的汽车网联化逐渐成为未来汽车的重要发展方向。联网所带来的信息安全问题在网联化汽车上同样存在，车厂和设计开发人员将不得不在整车电子电气架构上实施高要求的信息安全措施。2009 年欧洲的奥迪和宝马等汽车制造商发布了 Security Hardware Extension(SHE)标准(图 1)，2011 年由一些主要的 Tier 1 和汽车半导体公司发布基于 SHE 规范的 HSM 硬件规范，2016 年 SAE 针对车辆的生产、运行、维护和报废的整个生命周期。发布了提供了车辆网络安全的流程框架和指导 SAE J3061.2020， ISO 21434 是基于 SAE J3061 制定的、针对车辆整个生命周期的标准。这将是和 ISO 26262 功能安全一样的重量级的标准。

Intelligent connected vehicles are booming in the world, and the resulting automobile network connection has gradually become an important development direction of future automobiles. The same information security issues brought about by networking also exist in connected vehicles, and automakers and design developers will have to implement demanding information security measures in the vehicle electronic and electrical architecture. In 2009, European automakers such as Audi and BMW released the Security Hardware Extension(SHE) standard (Figure 1), and in 2011, some major Tier 1 and automotive semiconductor companies released HSM hardware specifications based on the SHE specification. The 2016 SAE addresses the entire life cycle of production, operation, maintenance, and obsolescence of vehicles.

Published SAE J3061.2020, a process framework and guidance for vehicle cybersecurity, ISO 21434 is a standard based on SAE J3061 for the entire vehicle lifecycle. This would be the same heavyweight standard as ISO 26262 for functional safety.

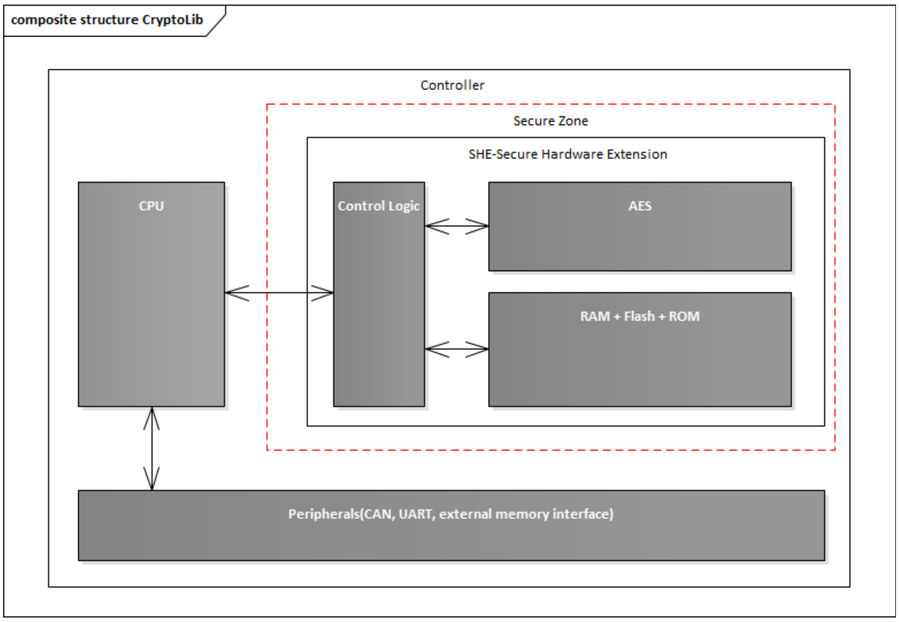

composite structure CryptoLib
Controller
Secure Zone
SHE-Secure Hardware Extension
CPU
Control Logic
AES
RAM + Flash + ROM
Peripherals(CAN, UART, external memory interface)

图 1 Secure Hardware Extension

Figure 1 Secure Hardware Extension

2018 年底，知从科技开始投入资源开发满足 SHE 标准并能兼容 AUTOSAR 4.2.2/4.4.0 的 HSM 内核和接口函数，经过不懈努力，终于 2020 年 9 月发布了基于英飞凌 TC3xx 的第一款信息安全软件库--木牛 CryptoLibrary。

At the end of 2018, ZC began to invest resources to develop the HSM kernel and interface functions that meet the SHE standard and are compatible with AUTOSAR 4.2.2/4.4.0. After unremitting efforts, the first information security software library based on Infineon TC3xx was finally released in September 2020 - MuNiu CryptoLibrary.

2 产品概述 PRODUCT OVERVIEW

知从科技针对英飞凌 TC3xx 系列(如 TC39x,TC38x 和 TC37x 等)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、ECDSA 和 ED25519 等。SHE CD 接口函数除了满足支持 AUTOSAR4.2.2 的需求外，还可升级到更高版本的 AUTOSAR 4.4.0,甚至可以作为一个单独的复杂驱动，和非 AUTOSAR 环境集成。

The MuNiu CryptoLibrary developed by ZC for Infineon's TC3xx series (such as TC39x, TC38x, TC37x, etc.) includes the kernel firmware (zHSM CORE) of the Hardware Security Module (HSM) and the customer application interface functions (SHE CD). Besides meeting the regular SHE functions (key injection, symmetric encryption and decryption, Message Authentication Code generation and verification, random number generation, and secure boot, etc.), the kernel firmware can also be extended with various algorithms, such as HASH, ECC256, ECDSA, and ED25519. In addition to meeting the requirements of AUTOSAR4.2.2, the SHE CD interface functions can be upgraded to the higher - version AUTOSAR 4.4.0. Moreover, it can even be integrated as a separate complex driver in a non - AUTOSAR environment.

简而言之，木牛 CryptoLibrary 灵活地适用于所有 AURIX 2G 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, MuNiu CryptoLibrary is flexibly applicable to all AURIX 2G products. It has high expandability, can be upgraded, configured and re - developed according to different customer project requirements, and ultimately meet the information security needs of different 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。 如图 2， 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。

MuNiu CryptoLibrary is mainly applied to controllers with information security requirements. As shown in Figure 2, this product is suitable for the following components in the automotive electrical and electronic architecture: Powertrain Domain Controller, Body Domain Controller, Safety Domain Controller, and Information Domain Controller.

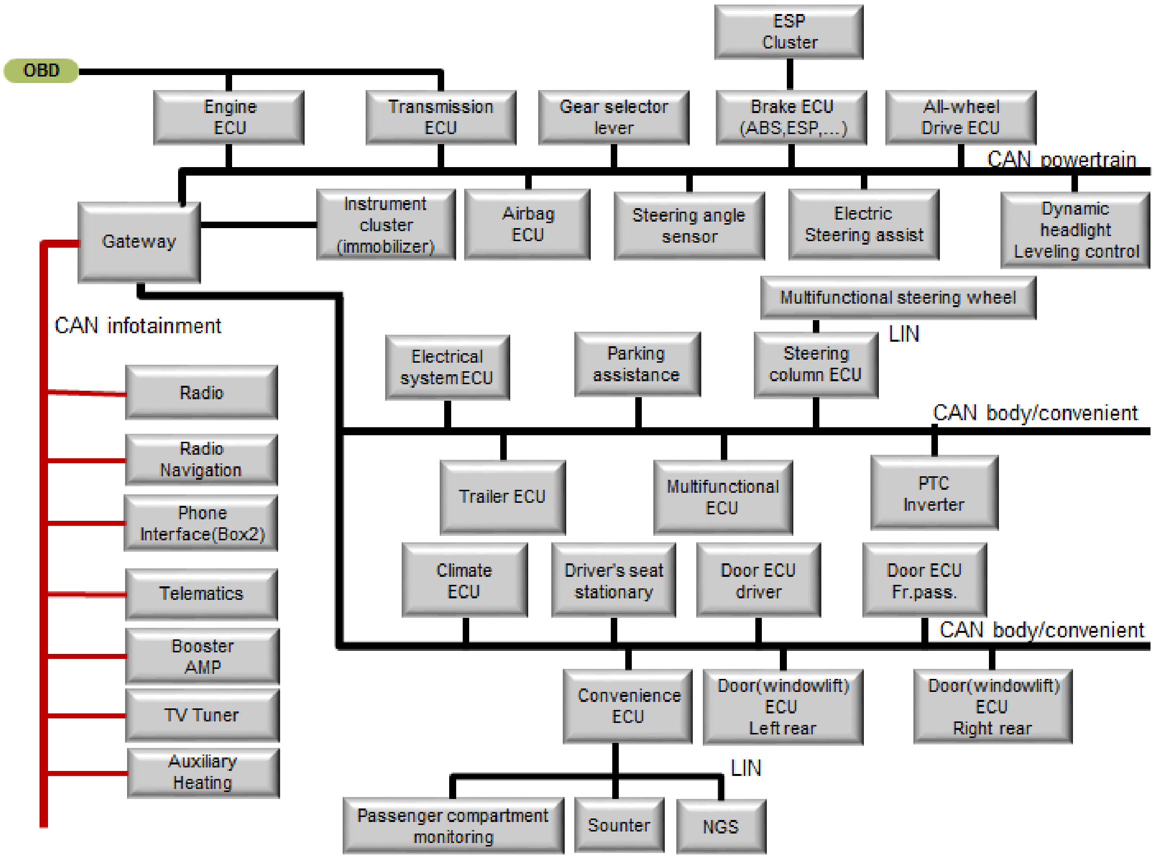


图 2 汽车电子电气架构

Figure 2 Automotive Electrical and Electronic Architecture

用户通过将木牛 CryptoLibrary 集成到基于 TC3xx 的汽车电控单元中， 可以满足 SHE 标准里所规定的汽车电控单元所具有的信息安全功能。

Users can meet the information security functions required for automotive electronic control units as specified in the SHE standard by integrating MuNiu CryptoLibrary into TC3xx - based automotive electronic control units.

4 软件模块及功能 SOFTWARE MODULES AND FUNCTIONS

木牛 CryptoLibrary 的软件主要分为两部分(图 3):

The software of MuNiu CryptoLibrary is mainly divided into two parts (Figure 3):

1) HSM 硬件加密模块固件(zHSM CORE)

Firmware of HSM (Hardware Security Module) (zHSM CORE)

2) Tricore 主核的 SHE 复杂驱动(zSHE CD)

SHE Complex Driver for Tricore Main Core (zSHE CD)

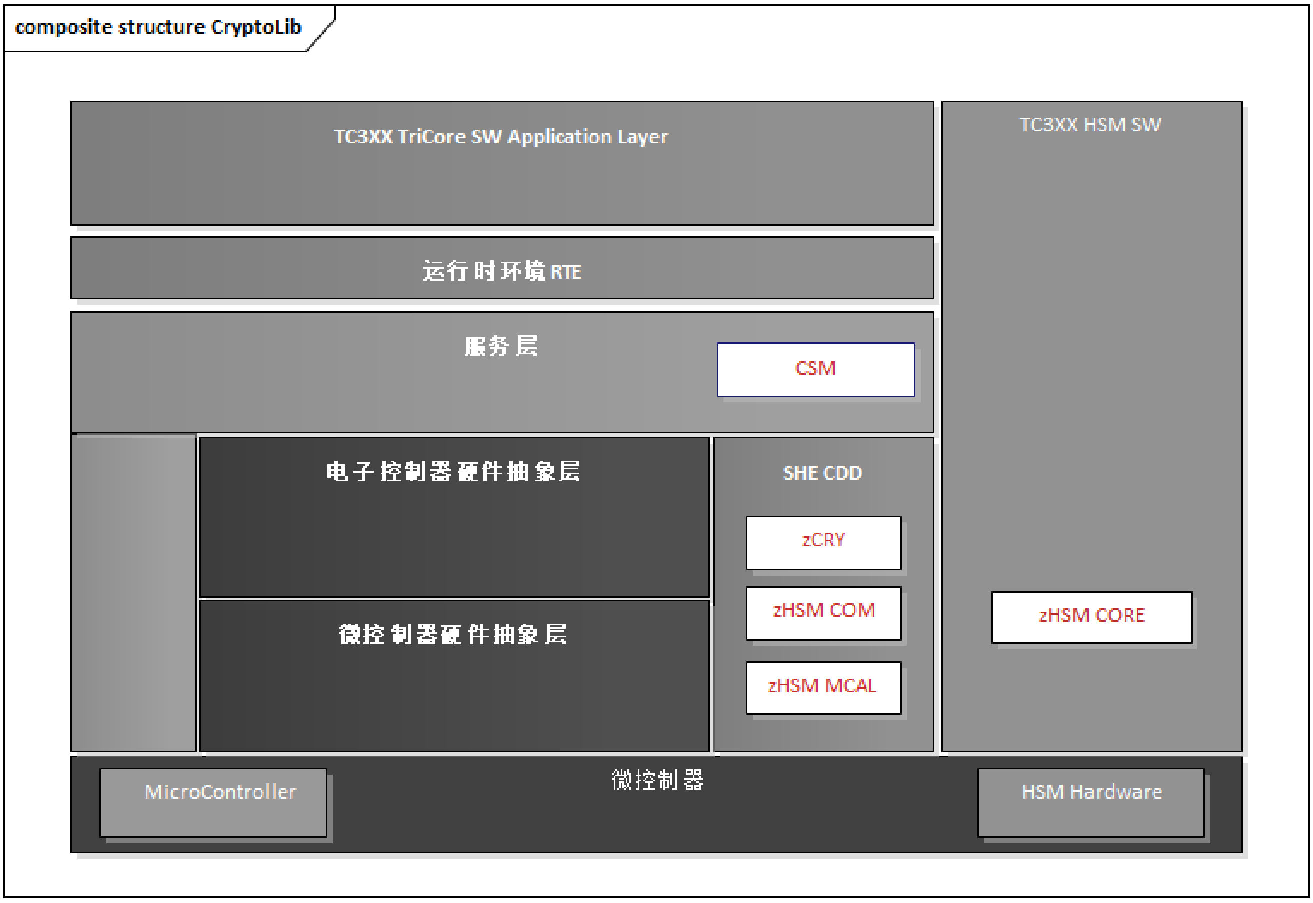


图 3 木牛 CryptoLibrary 的 AUTOSAR 集成

Figure 3 AUTOSAR Integration of MuNiu CryptoLibrary

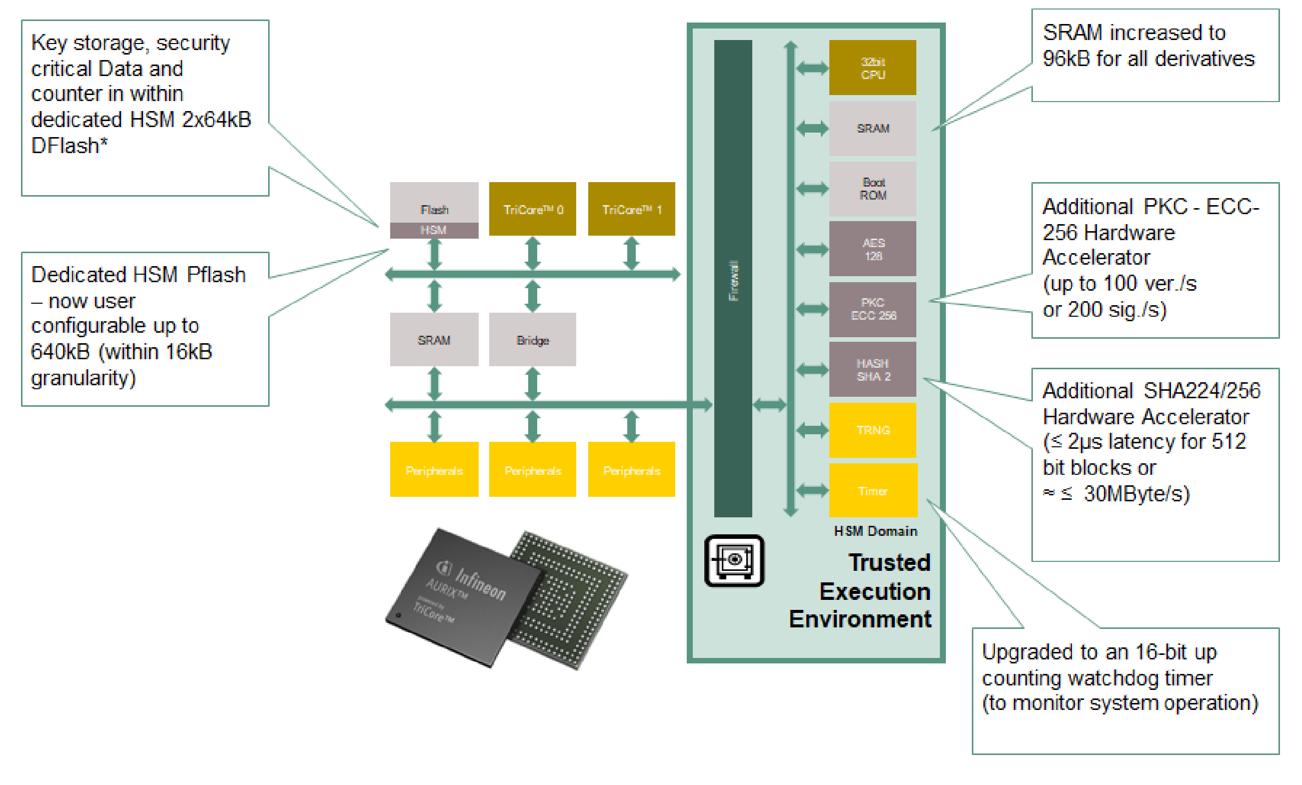
zSHE CD 包含和 CSM 的接口 zCRY 模块, 和 HSM 通讯的 zHSM COM 和 zHSM MCAL 模块三个子模块，各模块的功能介绍如表 1。

The zSHE CD contains three sub - modules: the zCRY module which is the interface with CSM, the zHSM COM and the zHSM MCAL module which communicate with HSM. The function 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 Function 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） It utilizes the hardware accelerators within the HSM, such as the random number generator, AES - 128, etc. (as shown in Figure 4).
zSHE CD （主核） (Main Core)	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 Microprocessor Hsm driver, communication driver with Hsm core, Crypto Interface, etc.
CSM （主核） (Main Core)	CSM	SERVICE	用户信息安全管理的接口函数 Interface functions for user information security management



Key storage, security critical Data and counter in within dedicated HSM 2x64kB DFlash*

Dedicated HSM Pflash – now user configurable up to 640kB (within 16kB granularity)

SRAM increased to 96kB for all derivatives

Additional PKC - ECC-256 Hardware Accelerator (up to 100 ver./s or 200 sig./s)

Additional SHA224/256 Hardware Accelerator (≤ 2μs latency for 512 bit blocks or ≈ ≤ 30MByte/s)

Upgraded to an 16-bit up counting watchdog timer (to monitor system operation)

图 4 TC3xx HSM 资源

Figure 4 TC3xx HSM Resources

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。

MuNiu CryptoLibrary supports the SHE standard. Compared with the standard SHE, CryptoLibrary has some functional expansions. 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 MuNiu CryptoLibrary

Features		SHE standard	木牛 CryptoLibrary MuNiu CryptoLibrary
AES 128 密码模式 AES 128 Cipher Modes	ECB	✓	✓
	CBC	✓	✓
AES 128 消息认证码 AES 128 Message Authentication Code	CMAC	✓	✓
随机数生成器 Random Number Generator	伪随机数 Pseudorandom 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		✓	✓

支持可用于消息认证密钥 Support for keys that can be used for message authentication.		/	✓
安全消息认证 Secure Message Authentication		/	✓
非对称加密 Asymmetric encryption	ECDSA	/	✓
	ED25519	/	✓
	Curve25519 / X25519	/	✓
密钥协商 Key negotiation	ECDH	✓	✓
	KDF	✓	✓
X509 证书 X.509 certificate	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 and Private Key Storage	/	✓
	Custom Extension 支持 Custom Extension Support	/	✓
国密算法	SM2	/	✓

National Cryptography Algorithm	SM3	／	✔
	SM4	／	✔

表 3 木牛 CryptoLibrary 的 SHE 功能说明

主要功能 Main functions	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, supporting ECB and CBC encryption modes for symmetric encryption.
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 SHE CMAC Secure Message Authentication Code Generation and Verification	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 the 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 exported RAM key.
SHE 基于安全协议的密钥装载 SHE Key Loading Based on Security Protocols	使用安全协议将 128 位密钥存储在 HSM 非易失性存储器中 Use a security protocol to store a 128 - bit key in the non - volatile memory of the HSM.
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.

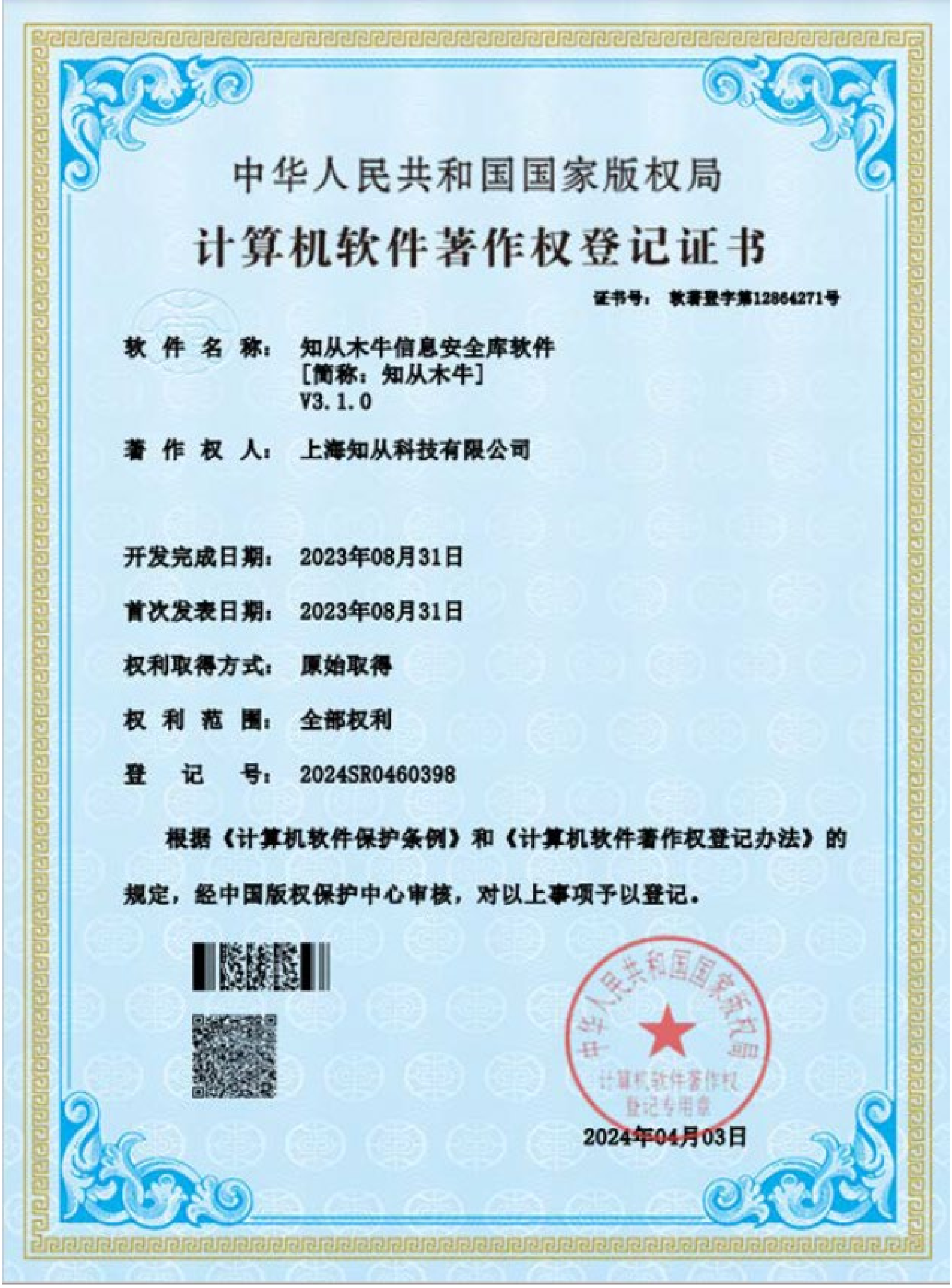
SHE 状态获取 SHE Status Retrieval	获取 SHE 状态. Obtain the SHE status.
SHE 命令取消 SHE Command Cancellation	取消当前正在执行的操作. Cancel the currently executing operation.
SHE 错误报告 SHE Error Reporting	除了 CSM 返回代码之外，还可以通过 AUTOSAR 机制报告 SHE 错误 In addition to the CSM return code, SHE errors can also be reported through the 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 Report an error if the HSM response time exceeds the predefined limit.
应软件更新支持 (Cipher 和 MAC) Support for Software Update (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 The cipher and MAC functions can also be used during the update process of the application software.
硬件随机数 Hardware Random Number	支持生成真随机数 Supports the generation of true random numbers.
AES 加密扩展 (OFB, CFB, CTR, XTS,GCM) AES Encryption Extension (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 extension of more non - volatile keys.

5 配置环境 CONFIGURATION ENVIRONMENT

配置环境 Configuration Environment	
硬件 (支持芯片) **Hardware (Supported Chips)**	INFINEON SAK-TC3XX
编译器选择 **Compiler Selection**	TASKING 6.2R2 TASKING 6.3R1 HighTec 4.9.3.0
评估硬件 **Evaluation Hardware**	TriBoard TC3xx
调试器 **Debugger**	Lauterbach (Trace32 XXXXX) Isystem (IC5XXX) PLS (UDE 5.X)
配置工具 **Configuration Tool**	Muniu_v5.0.5
配置环境 **Configuration Environment**	Win10 64bit/Win7 64bit

编译器选项 Configuration Environment	
Tasking 编译选项 Tasking Compilation Options	--core=tc1.6.2 -t -Wa-gAHLs --emit-locals=-equ,-symbols -Wa-Ogs -Wa--error-limit=42 $(ISO_OPTION) --eabi-compliant --integer-enumeration --language=-comments,-gcc,+volatile,-strings --switch=auto --align=0 --default-near-size=0 --default-a0-size=0 --default-a1-size=0 O<*variants*> --tradeoff=4 -g --source -D_TASKING_C_TRICORE_=1
Tasking 链接选项 Tasking Linking Options	-o "$(ELFDIR)/$(PROJNAME).elf" -o "$(ELFDIR)/$(PROJNAME).hex":IHEX --hex-format=s -t -D__CPU__=$(CPU_USED) -Cmpe:vtc $(LTC_OPTIMIZATION) --error-limit=42 -M -mcrfiklsmnoduq
HighTec 编译选项 HighTec Compilation Options	-save-temps=obj $(ISO_OPTION) -ansi -fno-asm -ffreestanding -Wundef -Wp,$(ISO_OPTION) -fno-short-enums -fpeel-loops -falign-functions=4 -frecord-gcc-switches -fsection-anchors -funsigned-bitfields -ffunction-sections -fno-ivopts -fno-peephole2 -nostartfiles -O3 -g3 -W -Wall -Wuninitialized $(TRIBOARD_DEFINE) -mtc162 -D_GNU_C_TRICORE_=1 $(CALLFUNCTION) -I "$(PRODDIR)/tricore/include/machine"
HighTec 链接选项 HighTec Linking Options	-o "$(ELFDIR)/$(PROJNAME).elf" -Wl,-Map="$(ELFDIR)/$(PROJNAME).map" -nostartfiles -Wl,--allow-multiple-definition -Wl,--cref -Wl,--oformat=elf32-tricore -Wl,--mcpu=tc162 -Wl,--mem-holes -Wl,--extmap="a" -L"$(PRODDIR)/tricore/include "

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12864271号

软 件 名 称：知从木牛信息安全库软件
［简称：知从木牛］
V3. 1. 0

著 作 权 人：上海知从科技有限公司

开发完成日期：2023年08月31日

首次发表日期：2023年08月31日

权利取得方式：原始取得

权 利 范 围：全部权利

登 记 号：2024SR0460398

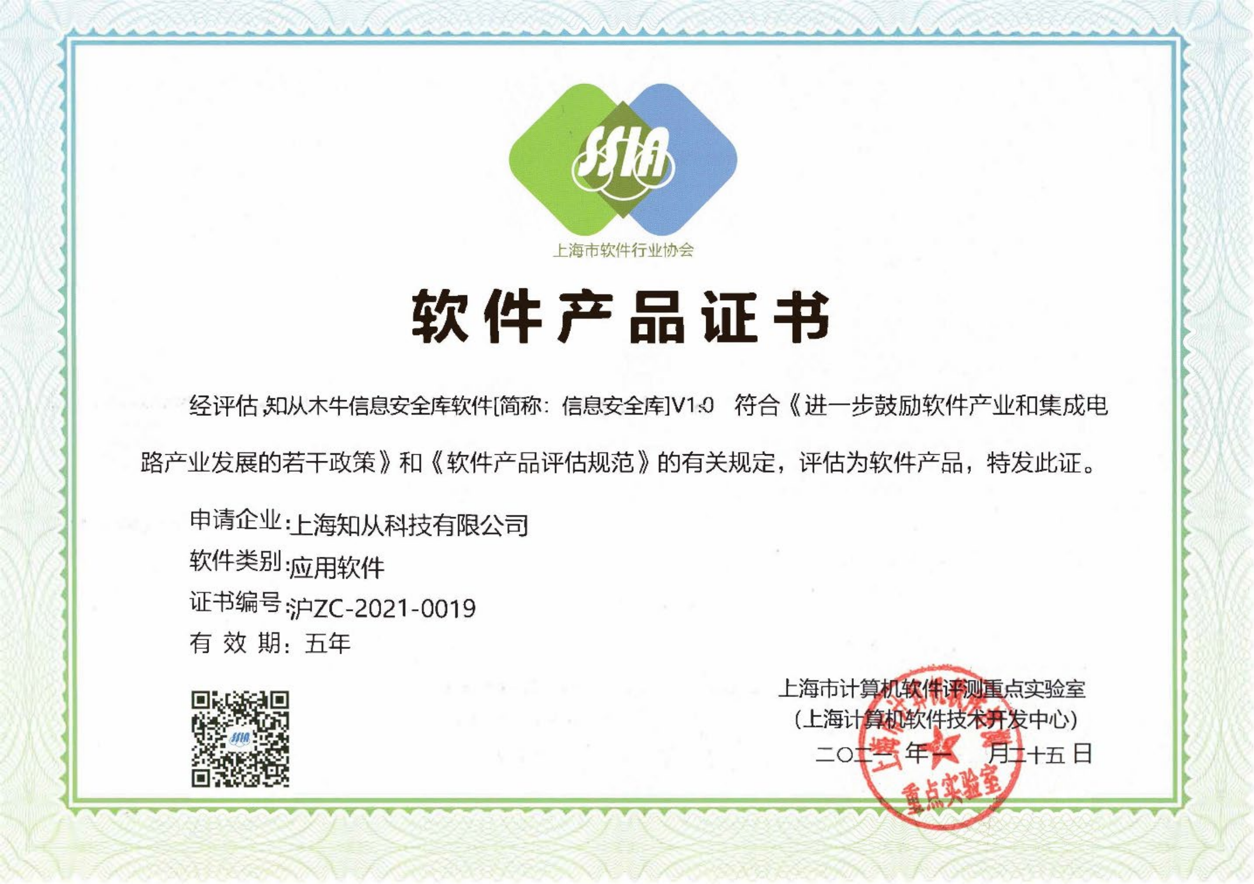
根据《计算机软件保护条例》和《计算机软件著作权登记办法》的规定，经中国版权保护中心审核，对以上事项予以登记。

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04月03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

木牛软件产品证书

CERTIFICATE OF REGISTRATION OF MU NIU SOFTWARE PRODUCT