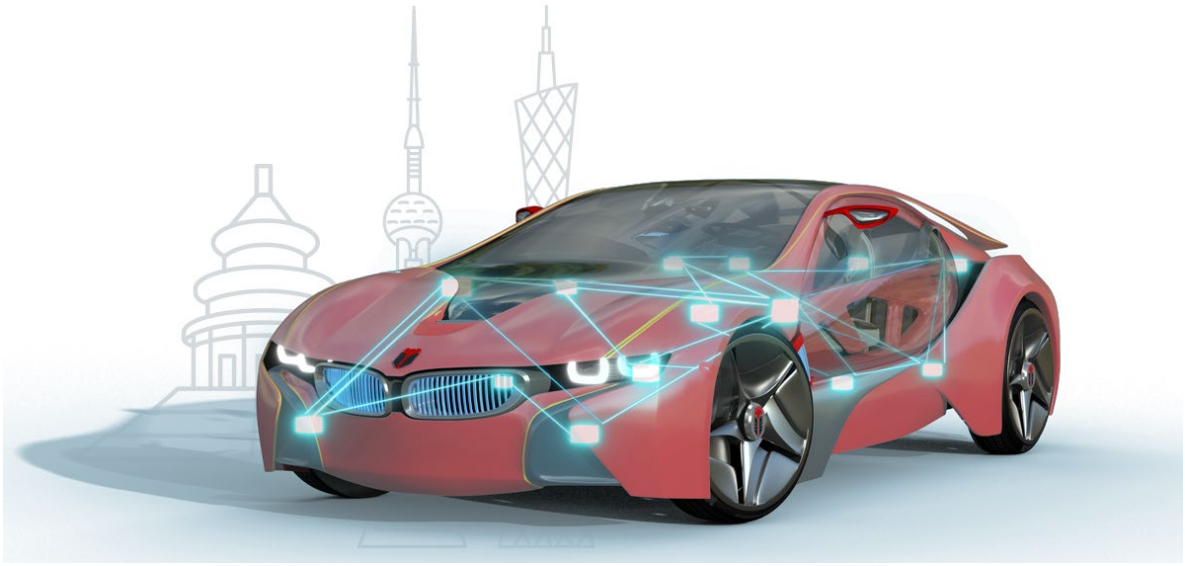
知从青龙 SECUREBOOT 英飞凌 TC377 产品手册
ZC.QINGLONG SECUREBOOT PRODUCT MANUAL BASED ON INFINEON TC377

知从青龙 BootLoader

ZC.QingLong BootLoader



知从青龙 SECUREBOOT 英飞凌 TC377 产品手册
ZC.QINGLONG SECUREBOOT PRODUCT MANUAL BASED ON INFINEON TC377

知从青龙 BootLoader
ZC.QingLong BootLoader

1 功能概述 FUNCTIONAL OVERVIEW

知从青龙 BootLoader 是由知从科技自主研发的程序刷新软件(BootLoader)。使用知从青龙 BootLoader 的控制器，可以通过 CAN、LIN、SPI、UART 等通信方式实现应用程序的更新功能。目前，知从青龙 BootLoader 已支持 NXP、Infineon、Renesas、ST 等多家芯片，并且支持多家整车厂程序刷新规范，可提供定制开发服务。

ZC.QingLong BootLoader is a self-developed program flashing software (BootLoader) by ZC. Controllers using ZC.QingLong BootLoader can achieve application update functionality through communication methods such as CAN, LIN, SPI, and UART. Currently, ZC.QingLong BootLoader has supported chips from NXP, Infineon, Renesas, ST, and more, and complies with the program flashing specifications of various vehicle manufacturers, offering customized development services.

知从青龙 SecureBoot 是基于 IFX TC3xx 平台，实现 BootLoader 的 Security 功能。通过实现 SecureBoot，控制器可以识别 BootLoader 程序和应用程序是否被篡改，特别是在 FOTA 过程中，可以保证程序刷新的安全性。通过实现 SecureUpdate，控制器可以在刷写过程中对交互数据进行加密，保证数据的安全性及有效性。通过 SecureDiagnostic，控制器通过上位机交互认证流程，确保 ECU 内数据不会被窃取，保证控制器的数据安全。

ZC.QingLong SecureBoot is based on the IFX TC3xx platform and implements the Security features of the BootLoader. By implementing SecureBoot, the controller can recognize whether the BootLoader program and the application have been tampered with, especially during the FOTA process, ensuring the security of the program update. By implementing SecureUpdate, the controller can encrypt the interactive data during the flashing process, ensuring the security and effectiveness of the data. Through SecureDiagnostic, the controller ensures that the data within the ECU is not stolen by interacting with the upper computer through an authentication process, thus ensuring the data security of the controller.

2 应用领域 APPLICATION FIELD

知从青龙 SecureBoot 可应用于使用 TC3xx 系列芯片的控制器程序刷新功能。支持的控制器包括:

ZC.QingLong SecureBoot can be applied to the controller program flashing function using the TC3xx series chips. The supported controllers include:

- 车身控制器 Body Controller
- 网关控制器 Gateway Controller
- 车载娱乐系统控制器 In-Vehicle Infotainment System Controller
- 电子驻车制动系统 Electronic Parking Brake System
- 胎压监测系统 Tire Pressure Monitoring System
- 电池管理系统 Battery Management System
- 空调控制系统 Air Conditioning Control System
- 车窗控制系统 Window Control System
- 门控系统 Door Control System

3 配置环境 CONFIGURATION ENVIRONMENT

配置环境 Configuration Environment	
Hardware (Chip)	TC377TP
Compilers Supported	Tasking v6.2r2 Tasking v6.3r1
Evaluation Hardware	Customer board / TC377TP demo board
Debugger	Lauterbach (Trace32 R.2023.02) Isystem (IC5700)
Configuration Tools	Muniu_v5.0.5
Configuration Environment	Win10 64bit

S32DS 编译器选项 S32DS Compiler Options	
编译选项 **Compiler Options**	-Ctc37x --lsl-core=vtc -t -Wa-H"sfr/regtc37x.def" -Wa-gAHLs --emit-locals=-equs,-symbols -Wa-Ogs -Wa--error-limit=42 -D_TASKING_C_TRICORE_=1 DNUMBER_OF_KEY_PAGES=5 -DAPP_SW=0 -DDEMO_APP=0 -DTEST_APP=1 --iso=99 --language=-gcc,-volatile,+strings,-kanji --integer-enumeration --fp-model=3 --switch=auto --align=0 --default-near-size=0 --default-a0-size=0 --default-a1-size=0 -O0 --tradeoff=4 -g --error-limit=42 --source
链接选项 **Linker Options**	-Ctc37x --lsl-core=vtc -t -Wl-o"${PROJ}.hex":IHEX:4 --hex-format=s "..\Linker\ZC_TC37x_TriCore.lsl" -Wl-OtxycL -Wl--map-file="${PROJ}.mapxml":XML -Wl-mcrfiklSmNOduQ -Wl--error-limit=42 -g --fp-model=3 --c++=03

4 开发背景 DEVELOPMENT BACKGROUND

目前，汽车上的电子电气架构越来越复杂，并伴随着汽车的电动化、智能化、网联化、共享化，软件的研发在汽车上占比越来越大。软件更新的频率越来越高。而且，在汽车的整个生命周期中，包括研发阶段、生产阶段、售后阶段，各个阶段都需要实现软件的更新功能。因此，客户对软件程序更新的需求越来越迫切。

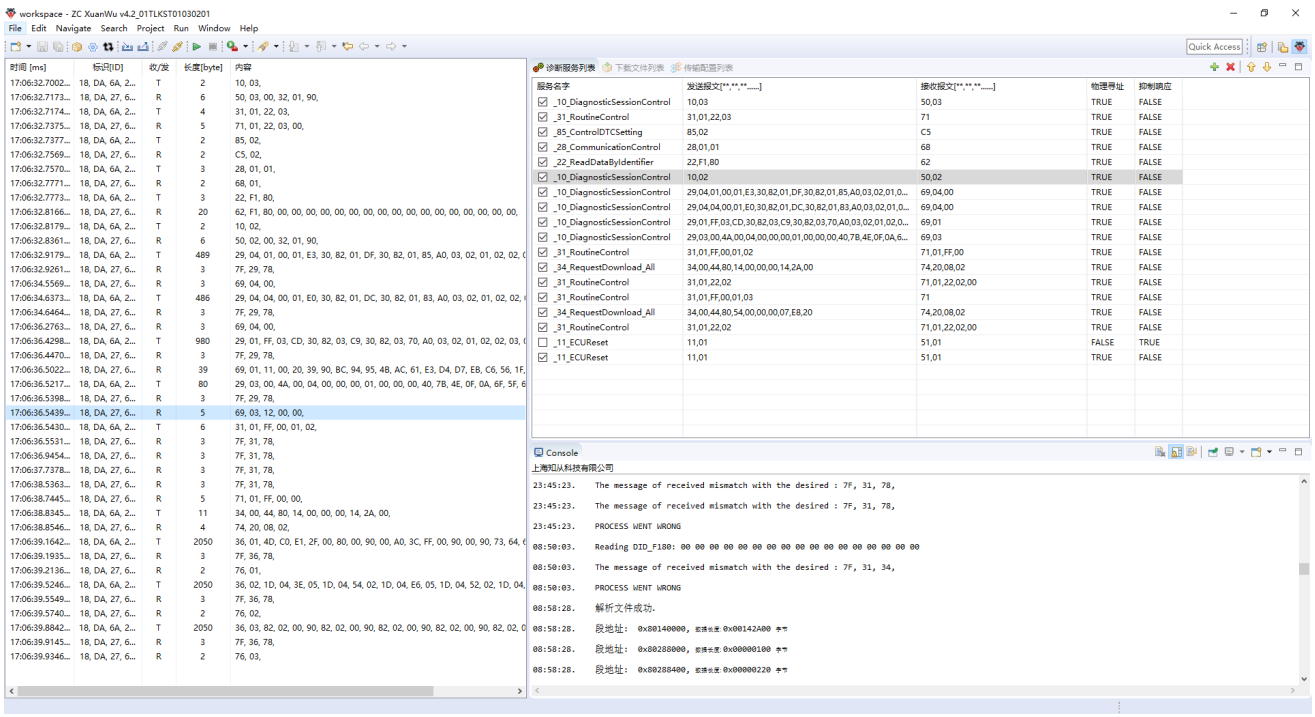
Currently, the electronic and electrical architecture of vehicles is becoming increasingly complex. Along with the electrification, intelligence, connectivity, and sharing of automobiles, the proportion of software development in vehicles is growing larger. The frequency of software updates is also increasing. Moreover, throughout the entire lifecycle of a vehicle, including the research and development phase, production phase, and after-sales phase, software update functionality is required in each stage. Therefore, the requirements from customers for software program updates is becoming more urgent.

并且，随着车联网的落地，信息安全越来越受重视，芯片作为信息的载体，因此，对芯片中的数据保护尤其重要。知从青龙 SecureBoot 是基于 Infineon TC3xx 平台，实现 BootLoader 的 Security 功能。通过实现 SecureBoot，控制器可以识别 BootLoader 程序和应用程序是否被篡改，特别是在 FOTA 过程中，可以保证程序刷新的安全性。

With the implementation of the Internet of Vehicles, Cybersecurity is gaining more attention. As chips serve as carriers of information, the protection of data within chips is particularly important. ZC.QingLong SecureBoot is based on the Infineon TC3xx platform and implements the security features of the BootLoader. By implementing SecureBoot, the controller can recognize whether the BootLoader program and the application have been tampered with, especially during the FOTA process, which ensures the security of program updates.

5 功能描述 FUNCTIONAL DESCRIPTION

5.1 产品特点 Product Features



知从玄武—程序更新工具
ZC.XuanWu—Program Update Tool

- 适用于多达十几家整车厂的程序更新规范
  Applicable to the program update specifications of up to more than ten vehicle manufacturers
- 支持应用程序和数据的更新功能
  Supports update functions for applications and data.
- 支持 BootLoader 自更新功能
  Support BootLoader self-update function
- 支持 HIS 规范
  Compliant with HIS standards
- 支持 CAN/LIN/SPI/UART 等通信
  Support for CAN/LIN/SPI/UART communication
- 适配知从玄武程序更新工具，提供完整的程序更新解决方案
  Compatible with ZC.XuanWu program update tool, providing a complete program update solution

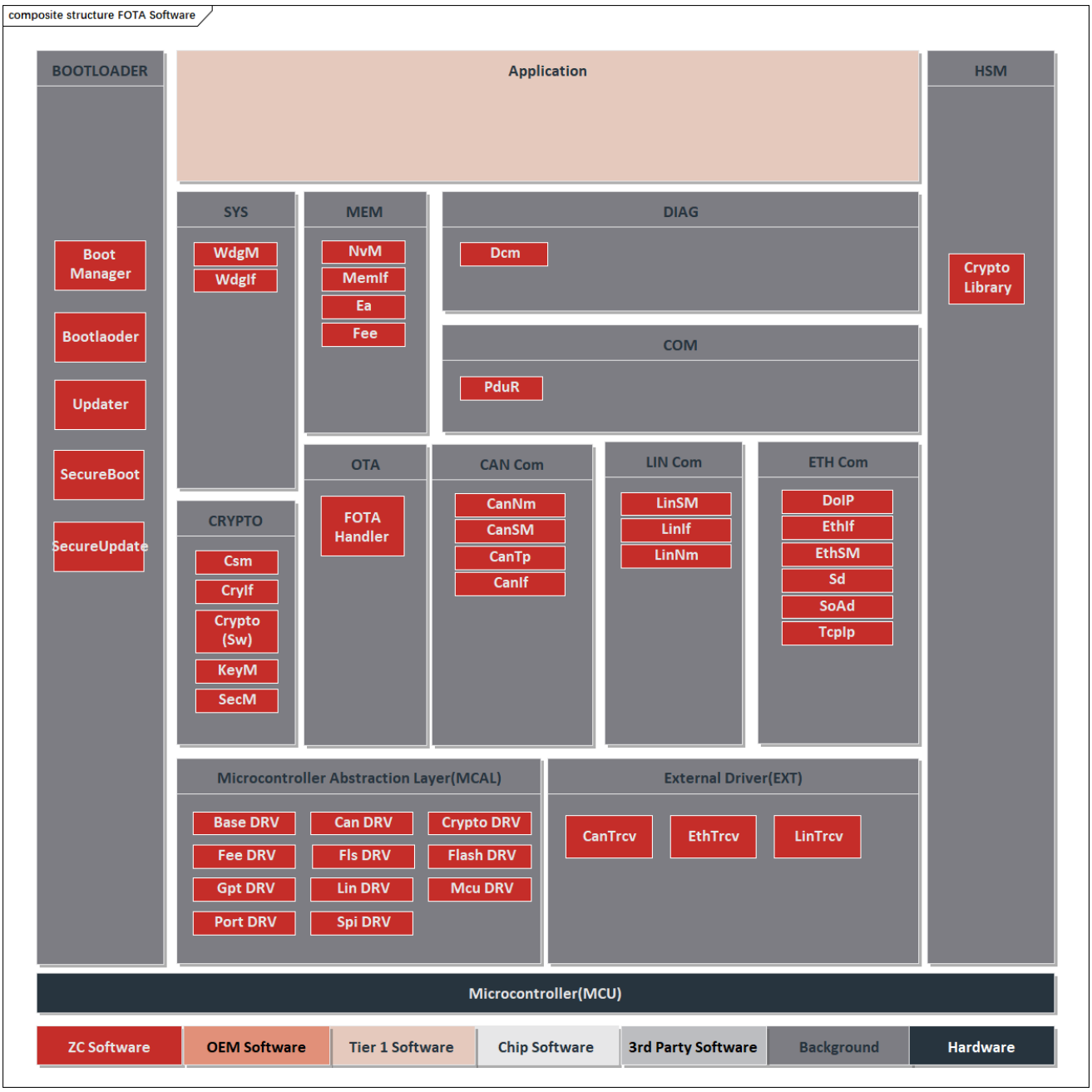
- 支持对称加密 SHA256 和 AES128 算法
  Support for symmetric encryption algorithms SHA256 and AES128

- 支持非对称加密 ECDSA 和 ED25519 算法
  Support for asymmetric encryption algorithms ECDSA and ED25519

- 支持 0x29, 0x84 服务
  Support for 0x29 and 0x84 services

- 支持证书解析, 签名验证
  Support for certificate parsing and signature verification

5.2 软件架构 Software Architecture



知从青龙 FOTA 系统架构支持 CAN、LIN、SPI、Ethernet 通信场景下的 FOTA 功能，通过 Dcm 模块实现 UDS 报文解析和诊断刷写，并通过适配 Crypto Library 实现各 OEM 规范的信息安全需求。以下为各模块的功能描述：

- Bootloader

  BootManager 模块提供 FOTA 启动管理功能，支持适配软硬件 SecureBoot 功能，通过烧录和刷写存储 Bootloader 和 Application 的期望 MAC 值，启动阶段 SecureBoot 通过计算比较 Bootloader 和 Application 的 MAC 执行软件完整性校验，保证软件安全需求。
- Can Com

  Can 模块支持 CAN、CANFD 通信功能。
- Spi Com

  Spi 模块支持主从刷写功能，通过适配 5、6、7 线硬件配置，可支持多种 SPI 通信刷写模式。
- Ethernet Com

  DoIP 模块基于 TCP/IP 协议实现 Ethernet 通信收发功能，满足 ISO 13400 标准定义。通过车辆识别、路由激活、诊断消息功能实现 UDS 刷写流程，实现 Ethernet OTA 功能。
- Dcm

  Dcm 模块基于通信模块支持实现诊断功能，满足 ISO 14229 以及 ISO 15765 标准定义。
- Crypto、HSM

  Ethernet OTA 支持适配木牛加密库功能，支持非对称加密算法和加密算法结合实现安全刷写功能，适配证书认证功能满足安全诊断功能，适配 HSM 提高信息安全功能的稳定性和校验速度。

The Qinglong Ethernet FOTA system architecture supports the FOTA function in communication scenarios such as CAN, LIN, SPI, and Ethernet. It realizes the parsing of UDS messages and diagnostic programming through the Dcm module, and meets the information security requirements of various OEM specifications by adapting to the Crypto Library. The following are the functional descriptions of each module:

- Bootloader

  The BootManager module provides FOTA startup management functions and supports the adaptation of hardware and software SecureBoot functions. It stores the expected MAC values of the Bootloader and Application through programming and flashing. During the startup phase, SecureBoot performs software integrity verification by calculating and comparing the MACs of the Bootloader and Application to ensure software security requirements.

- Can Com

  The Can module supports CAN and CANFD communication functions.

- Spi Com

  The Spi module supports the master-slave programming function. By adapting to the hardware configurations of 5, 6, and 7 wires, it can support multiple SPI communication programming modes.

- Ethernet Com

  The DoIP module realizes the Ethernet communication sending and receiving functions based on the TCP/IP protocol, meeting the definition of the ISO 13400 standard. It implements the UDS flashing process through vehicle identification, routing activation, and diagnostic message functions, thereby achieving the Ethernet OTA function.

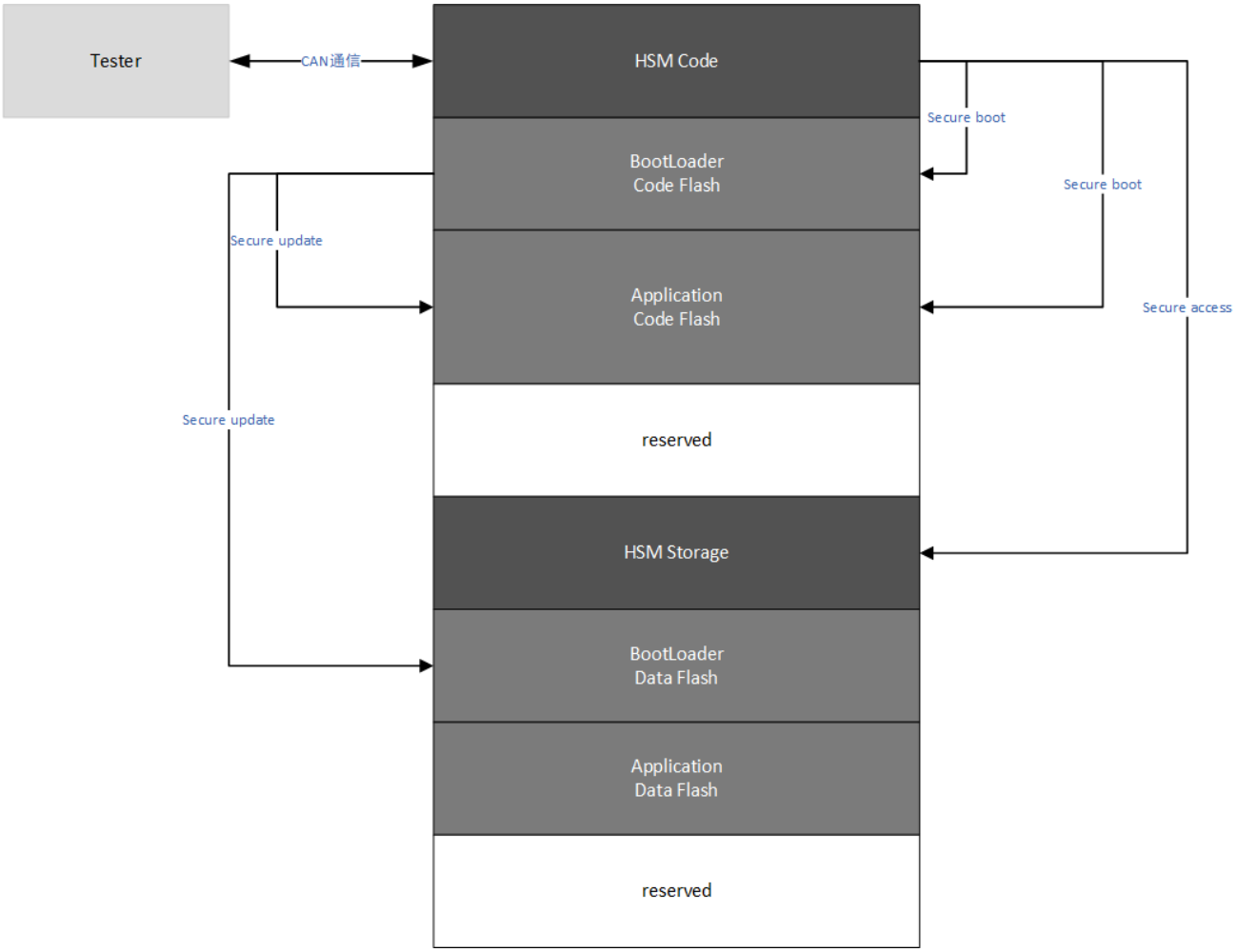
- Dcm

  The Dcm module realizes the diagnostic function based on the support of the communication module, meeting the definitions of ISO 14229 and ISO 15765 standards.

- Crypto, HSM

  The Ethernet OTA supports the adaptation of the Muniu Crypto Library functions. It combines asymmetric encryption algorithms with other encryption algorithms to achieve the secure flashing function. It adapts to the certificate authentication function to meet the security diagnostic requirements and adapts to the HSM to improve the stability and verification speed of the Cybersecurity function.

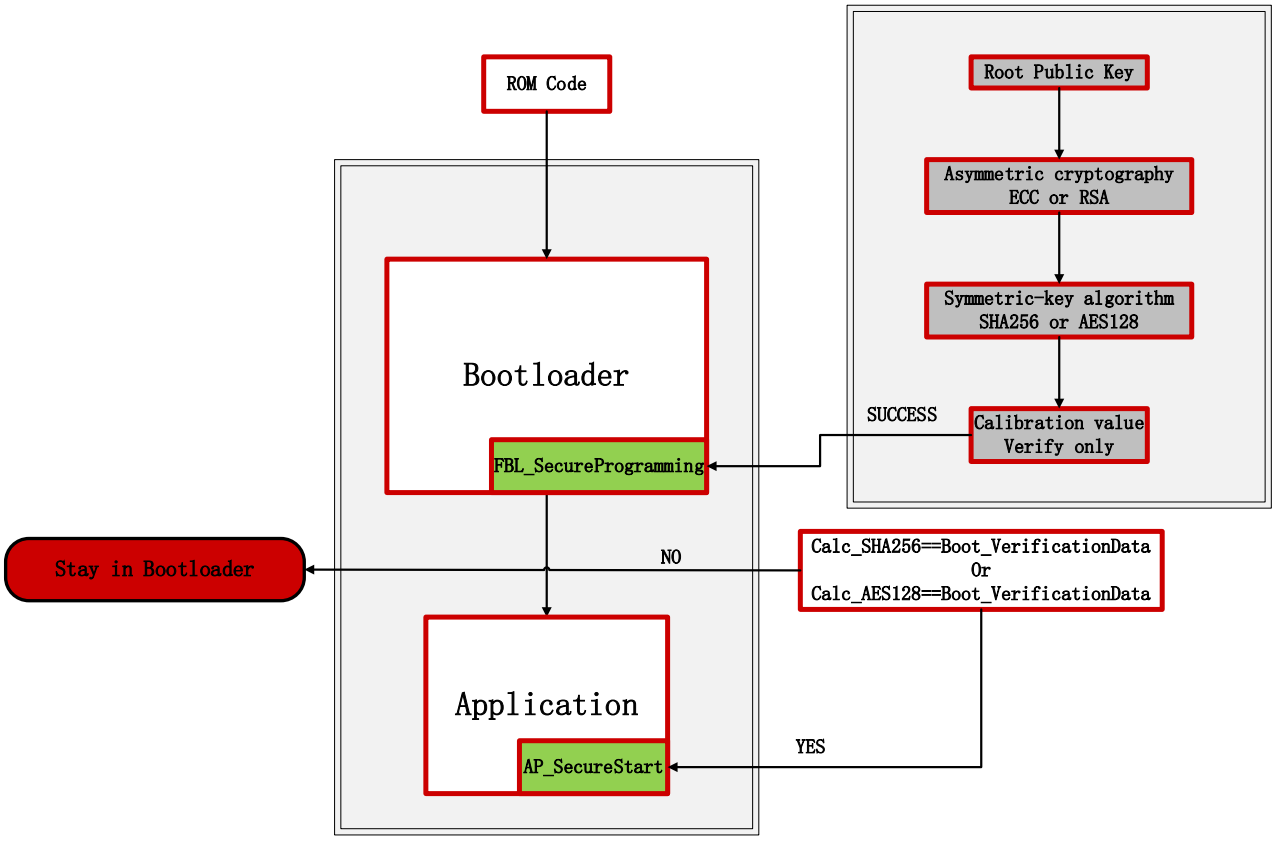
5.3 内存结构 Memory Structure



ECU 的内存分为 PFLASH 和 RAM，PFLASH 区分为 Application & Data，BootLoader 和 Hsm 区，RAM 区分为 FLASH Driver 和 Data。

The ECU's memory is divided into PFLASH and RAM. PFLASH is further divided into Application & Data, BootLoader, and Hsm areas. RAM is divided into FLASH Driver and Data areas.

5.4 安全刷写与安全启动 Secure Flashing and Secure Boot



知从青龙 SecureBoot 支持安全刷写与安全启动功能。

The ZC.QingLong SecureBoot supports secure flashing and secure boot functions.

➢ 安全刷写 Secure Flashing

知从青龙 SecureBoot 根据存储在非易失性存储器的 Root Public Key，通过非对称加密算法 ECC 或 ED25519，对数据的真实性校验。认证流程支持 0x29 服务，通过存储在 ECU 的证书校验上位机发送的 Client Certificate，若校验成功则允许进行后续的刷写流程，刷新过程通过对称加密算法 AES128 对数据进行加密，通过 SHA256 对数据进行完整性校验，保证刷写流程的安全性。

The ZC.QingLong SecureBoot verifies the authenticity of the data using the Root Public Key stored in non-volatile memory and employs asymmetric encryption algorithms ECC or ED25519. The authentication process supports the 0x29 service, which validates the Client Certificate sent by the host machine using the certificate stored in the ECU. If the validation is successful, the subsequent flashing process is allowed. During the flashing process, data is encrypted using the symmetric encryption algorithm AES128 and its integrity is verified using SHA256, ensuring the security of the flashing process.

- 安全诊断 Secure Diagnostics

知从青龙 SecureBoot 在进行诊断流程时,支持 0x29 服务，通过证书链校验保证上位机的真实性和有效性， 经过认证过程后，数据交互可通过对称加密进行数据加密， 其中加密秘钥通过秘钥派生算法生成，确保秘钥无法被中间人攻击及窃取。

When performing the diagnostic process, the ZC.QingLong SecureBoot supports the 0x29 service to ensure the authenticity and validity of the host machine through certificate chain verification. After the authentication process, data communication can be encrypted using symmetric encryption, with the encryption key generated through a key derivation algorithm to prevent key interception and theft by man-in-the-middle attacks.

- 安全启动 Secure Boot

芯片上电启动到跳转入 Application 的过程中，知从青龙 SecureBoot 支持安全启动功能，通过对称加密算法 SHA256 或 AES128 对 Boot 和 Application 应用程序进行安全验证，保证程序安全启动。

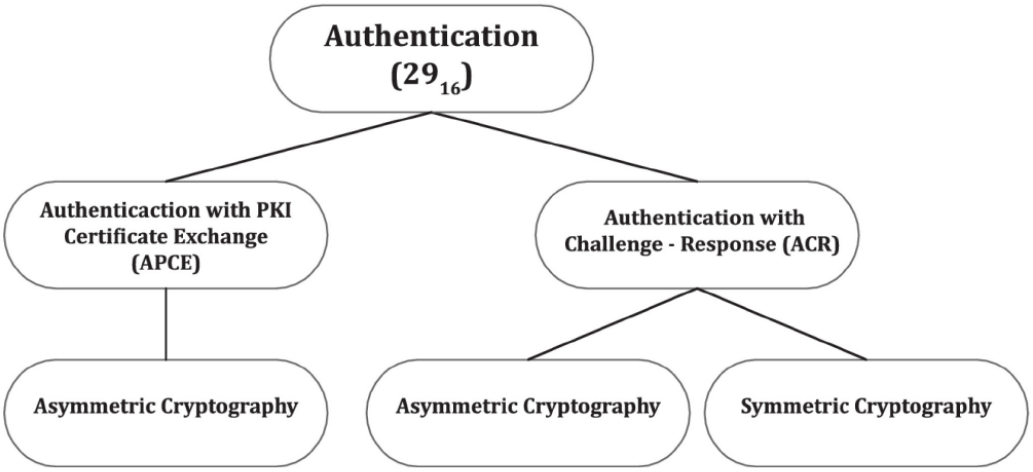
From the moment the chip is powered on and starts up until it jumps to the Application, the ZC.QingLong SecureBoot supports the secure boot function. It performs security verification on the Boot and Application programs using symmetric encryption algorithms SHA256 or AES128 to ensure the safe startup of the programs.

5.5 0x29 服务和 0x84 服务支持 Support for 0x29 and 0x84 Services

知从青龙 SecureBoot 支持 0x29 服务，基于 ISO14229-1:2020 标准；其中支持以下两种安全概念:

The ZC.QingLong SecureBoot supports the 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。
  Public Key Infrastructure (PKI) Certificate Exchange Process using 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。
  Challenge-Response Process without PKI Certificates: This involves using asymmetric cryptographic algorithms combined with software authentication tokens or symmetric keys, without the use of PKI certificates.



知从青龙 SecureBoot 支持 0x29 子服务列表:

ZC.QingLong SecureBoot supports the 0x29 sub-service list:

子服务 Sub-service	名称 Name	描述 Description
00	De Authenticate	此子服务有效地结束认证状态。 This sub-service effectively terminates the authentication status.
01	Verify Certificate Unidirectional	此子服务启动单向身份验证过程。 This sub-service initiates a one-way authentication process.
02	Verify Certificate Bidirectional	此子服务启动双向身份认证验证过程。 This sub-service initiates a two-way authentication process.
03	Proof Of Ownership	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 ownership proof data to the diagnostic tool.
04	Transmit Certificate	此子服务用于传递身份验证所需的证书链或 OCSP Response 信息。 This sub-service is used to transfer the certificate chain or OCSP Response information required for authentication.

知从青龙 SecureBoot 支持 0x84 服务，基于 ISO14229-1:2020 标准；其中支持以下功能点：

ZC.QingLong SecureBoot supports the 0x84 service, based on the ISO14229-1:2020 standard; it supports the following features:

- ✓ Anti-replay Counter： 防重复攻击
  Anti-replay Counter: Prevents replay attacks.
- ✓ Signature/MAC Byte：针对诊断服务进行前面计算，避免数据被中间人修改。
  Signature/MAC Byte: Calculates in advance for diagnostic services to prevent data from being modified by a man-in-the-middle.
- ✓ Encryption Calculation：通过对称加密，实现端到端数据安全，避免交互数据被中间人截取。
  Encryption Calculation: Uses symmetric encryption to ensure end-to-end data security, preventing interaction data from being intercepted by a man-in-the-middle.
- ✓ HKDF：支持秘钥派生算法，使用秘钥派生算法交互生成对称加密秘钥，有效加强秘钥安全性。
  HKDF: Supports key derivation algorithms. Using key derivation algorithms to interactively generate symmetric encryption keys effectively enhances key security.

6 过程文档 PROCESS DOCUMENTATION

开发流程 Development Process	文档描述 Document Description
需求收集 Requirement Collection	顾客的需求文档 Customer Requirement Document
软件需求分析 Software Requirement Analysis	需求分析 Requirement Analysis
	需求分析规格书 Requirement Analysis Specification
	软件需求追踪表 Software Requirement Traceability Matrix
	客户的问题沟通表 Customer Issue Communication Form
软件架构设计 Software Architecture Design	软件架构说明书 Software Architecture Manual
	软件架构的追踪表 Software Architecture Traceability Table
软件详细设计和单元设计 Software Detailed Design and Unit Design	BootLoader 详细设计说明书 BootLoaderBootLoader Detailed Design Manual
	配置工具设计 Configuration Tool Design
	软件详细设计追踪表 Software Detailed Design Traceability Table
	BootLoader 详细设计评审 BootLoader Detailed Design Review
软件单元测试 Software Unit Testing	QAC 分析报告 QACAnalysis Report
	Tessy 测试报告 Tessy Test Report
	软件单元验证策略 Software Unit Verification Strategy
软件集成和集成测试	集成策略 Integration Strategy

开发流程 Development Process	文档描述 Document Description
Software Integration and Integration Testing	集成手册 Integration Manual
	集成测试策略 Integration Test Strategy
	集成测试报告 Integration Test Report
	资源分析报告 Resource Analysis Report
软件系统测试 **Software System Testing**	BootLoader 软件测试报告 BootLoader BootLoader Software Test Report
	BootLoader 软件测试报告评审 BootLoader BootLoader Software Test Report Review
发布 **Release**	发布文档 Release Documentation

7 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3073051号

软件名称：知从青龙bootloader软件
[简称：青龙]
V1.0

著作权人：上海知从科技有限公司

开发完成日期：2018年01月04日

首次发表日期：2018年01月10日

权利取得方式：原始取得

权利范围：全部权利

登记号：2018SR743956

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
2018年09月13日

No. 02965607

青龙软件著作权登记证书
QINGLONG SOFTWARE COPYRIGHT REGISTRATION CERTIFICATE

中国软件产品评估 CSPE CSIA CHINA SOFTWARE PRODUCTS EVALUATION

软件产品证书

经评估，知从青龙bootloader软件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《软件产品评估标准》（T/SIA003 2017）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：沪RC-2019-3315
证书编号：嵌入式应用软件
有 效 期：五年

评估机构：上海市软件行业协会
日期：二〇一九 年 九 月 十五 日

上海市软件行业协会 软件产品评估证书专用章

青龙软件产品登记证书
QINGLONG SOFTWARE PRODUCT REGISTRATION CERTIFICATE