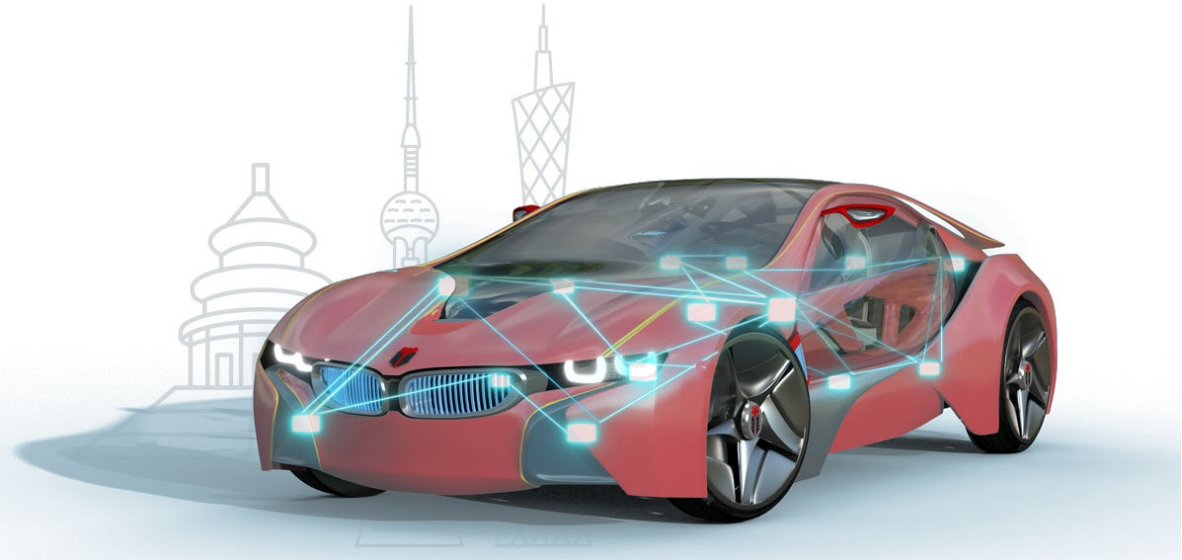
知从青龙 BOOTLOADER 英飞凌 TC213 SMTC 产品手册

ZC.QINGLONG BOOTLOADER PRODUCT MANUAL BASED ON INFINEON TC213 SMTC

知从青龙 BootLoader

ZC.QingLong BootLoader



知从青龙 BOOTLOADER 英飞凌 TC213 SMTC 产品手册

ZC.QINGLONG BOOTLOADER PRODUCT MANUAL BASED ON INFINEON TC213 SMTC

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 update software (BootLoader) by ZC. Using the controller of ZC.QingLong BootLoader, the application update function can be achieved through communication methods such as CAN, LIN, SPI, and UART. Currently, ZC.QingLong BootLoader has supported chips from multiple manufacturers like NXP, Infineon, Renesas, and ST, and it also supports the program update specifications of various vehicle manufacturers, providing customized development services.

此文档描述了知从青龙 BootLoader 基于 TC213 平台，实现对 SMTC 2 800 004、SMTC 2 800 007、SMTC 3 800 008 规范的支持。目前已实现支持等功能需求，满足 SMTC 规范中大部分的刷写需求。

This document describes the support for SMTC 2 800 004, SMTC 2 800 007, and SMTC 3 800 008 specifications based on the TC213 platform by ZC.QingLong BootLoader. It has already realized the support for the required functions and meets most of the writing needs in the SMTC specifications.

2 应用领域 APPLICATION FIELD

知从青龙 BootLoader 可应用于使用 TC213 系列芯片的控制器程序刷新功能。支持的控制器包括:

The ZC.QinLong BootLoader can be applied to the controller program update function that uses the TC213 series of chips. The supported controllers include:

- 车身控制器
  Body Control Module
- 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)	TC213
Compilers Supported	Tasking v6.2r2
Debugger	lsystem (IC5700)

Tasking 编译器 Tasking Compiler	
编译选项	-Ctc21x --lsl-core=vtc -t -I-Wa-H -I -Wa-gAHLs --emit-locals=-equs,-symbols -Wa-Ogs -Wa--error-limit=42 - --iso=99 --language=-gcc,-volatile,+strings,-kanji --fp-model=3 --switch=auto --align=0 --default-near-size=8 --default-a0-size=0 --default-a1-size=0 -O2 --tradeoff=4 --compact-max-size=200 -g --error-limit=42 --source
链接选项	-Ctc21x --lsl-core=vtc -t -I"D:\Git\ENSLC01\ENSLC01_TC213" -Wl-o"${PROJ}.hex":IHEX:4 --hex-format=s "../ENSLC01_TC213.lsl" -Wl-OtxycL -Wl--map-file="${PROJ}.mapxml":XML -Wl-mcrfiklSmNOduQ -Wl--error-limit=42 -g --fp-model=3

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。

At present, the electronic and electrical architecture of vehicles is becoming increasingly complex. Along with the electrification, intelligence, connectivity, and sharing of cars, 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 R&D phase, production phase, and after-sales phase, software update functionality is needed in every stage. Therefore, the demand for software program updates from customers is becoming more urgent.

对于整车厂或供应商，BootLoader 是控制器开发必备的功能。并且，不同的整车厂有不同的程序更新规范，同时 BootLoader 驱动又依赖于不同的芯片。因此，为了满足不同的整车厂程序更新规范，又适配不同的芯片，知从科技提供了完整的 BootLoader 解决方案—知从青龙 BootLoader。知从青龙 BootLoader 既适用于不同的整车厂程序更新规范，又适用于不同芯片厂商的芯片，让客户更专注与自己的控制器产品研发。

For vehicle manufacturers or suppliers, BootLoader is an essential feature for the development of controllers. Moreover, different vehicle manufacturers have different program update specifications, and BootLoader drivers depend on different chips. Therefore, to meet the various program update specifications of vehicle manufacturers and to be compatible with chips from different chip manufacturers, ZC provides a complete BootLoader solution—the ZC.QingLong BootLoader. The ZC.QingLong BootLoader is applicable to different vehicle manufacturer program update specifications and chips from various chip manufacturers, allowing customers to focus more on their own controller product development.

SMTC 平台架构在 BootLoader 中，通过实现 Secure Boot、签名旁路验证、安全刷写等功能，降低了在 MCU 更新过程中的安全风险，大幅提升了 BootLoader 的安全性以及可靠性。

The SMTC platform architecture, within the BootLoader, implements features such as Secure Boot, signature bypass verification, and secure flashing, which reduce the security risks during the MCU update process and greatly enhance the security and reliability of the BootLoader.

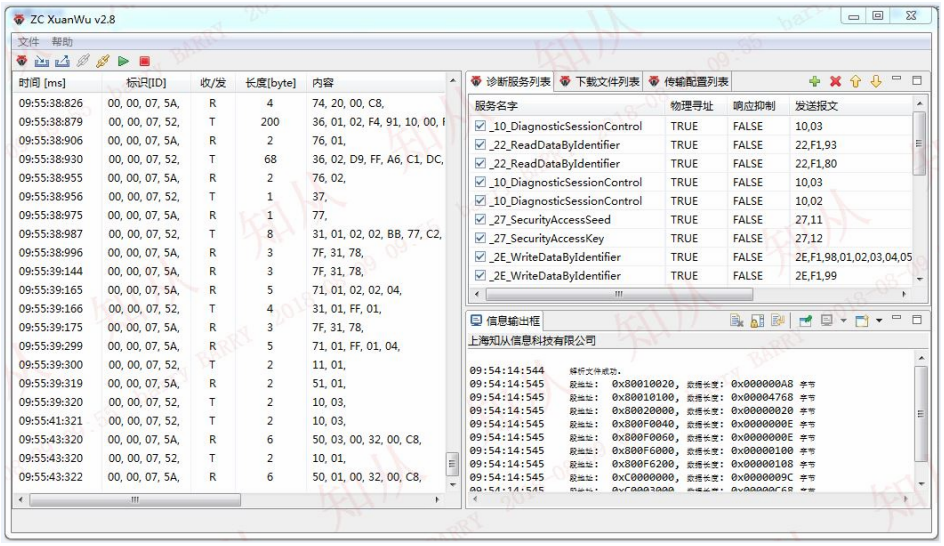
5 功能描述 FUNCTIONAL DESCRIPTION

5.1 产品特点 Feature Description

- 适用于 SMTC 平台规范 Compatible with SMTC Platform Specifications
- 支持应用程序和数据的更新功能 Supports application and data update functionality.
- 支持 CAN 等通信 Supports communication via CAN and other protocols.
- 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

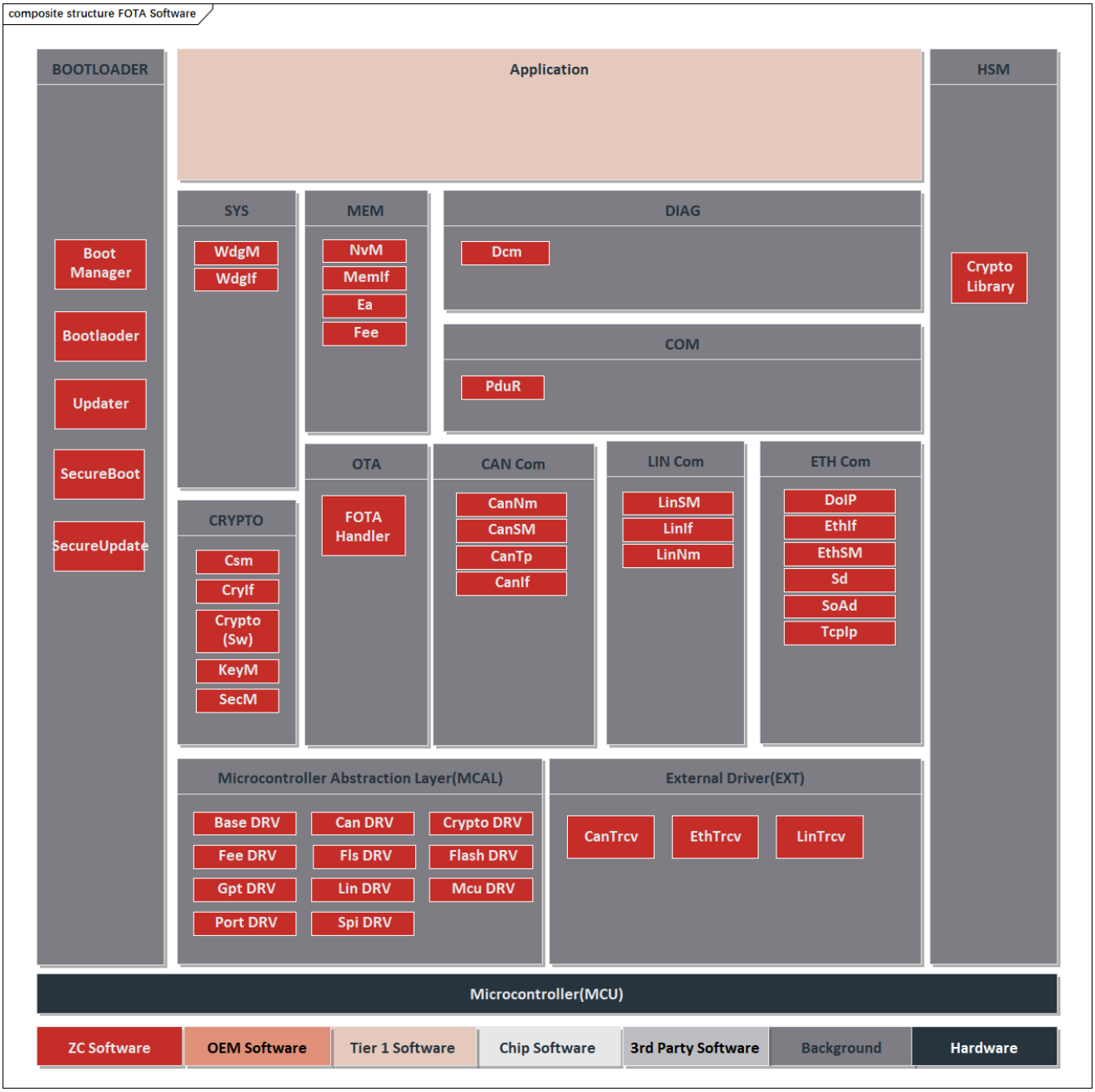
  Adapts to ZC.XuanWu program update tools, providing a complete program update solution.
- 支持对称加密 SHA256 算法 Supports the symmetric encryption algorithm SHA256.
- 支持非对称加密 ECC 算法

  Supports the asymmetric encryption algorithm ECC (Elliptic Curve Cryptography).
- 支持签名旁路认证功能 Supports signature bypass authentication function.
- 支持安全启动功能 Supports secure boot functionality.
- 支持安全刷写功能 Supports secure flashing functionality.



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

5.2 软件架构 Software Architecture



FOTA 系统架构
FOTA SYSTEM 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 和 BootLoader 区，RAM 区分为 FlashDriver 和 Data。

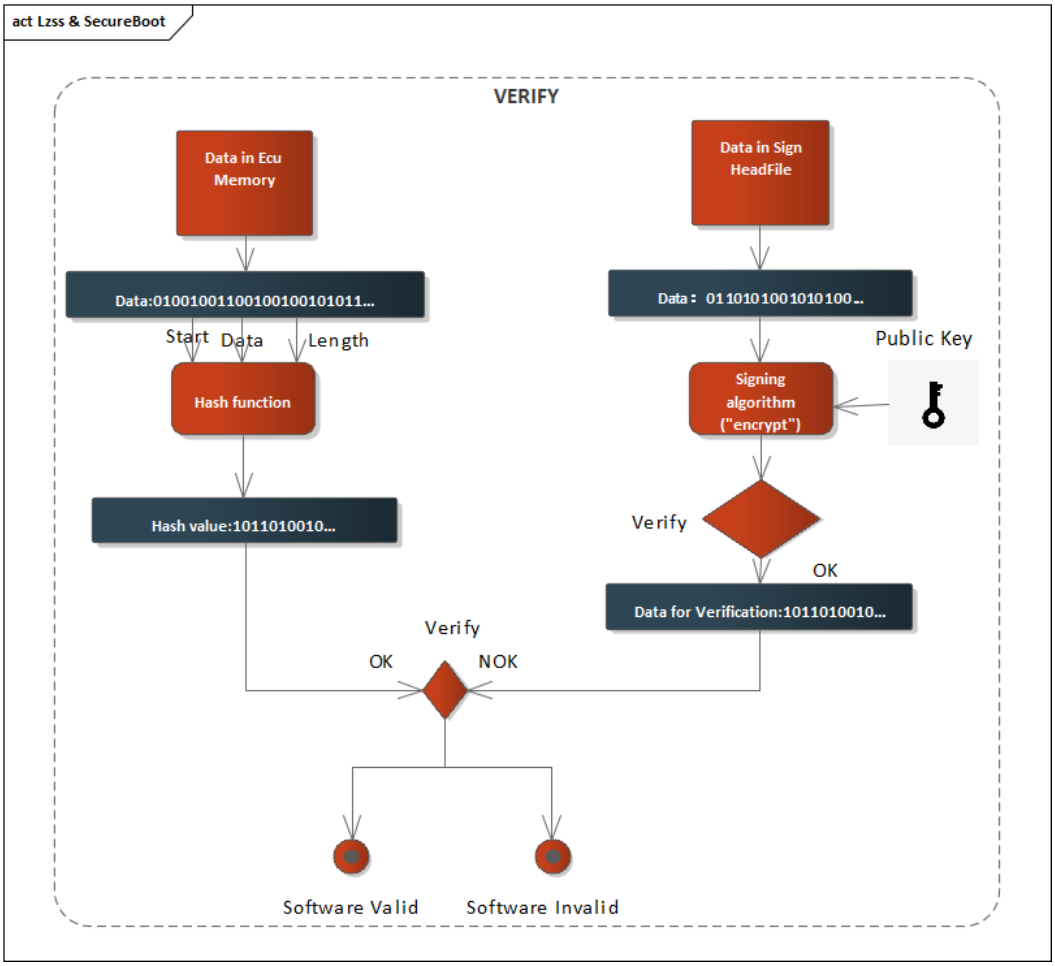
The memory of the ECU (Electronic Control Unit) is divided into PFLASH and RAM. The PFLASH is further divided into the Application & Data area and the BootLoader area. The RAM is divided into the FlashDriver area and the Data area.

5.4 支持 SMTC 规范 Supports SMTC Specifications.

- 安全刷写功能：
  Secure Flashing Feature：

知从青龙 BootLoader 支持 SMTC 规范的 SecureBoot 流程中的安全刷写功能，下图为简化示例图：

ZC.QingLong BootLoader supports the secure flashing feature in the SecureBoot process according to the SMTC specifications. The following is a simplified example diagram：



当 Bootloader 执行刷写流程时，Bootloader 会通过非对称加密算法和根公钥，校验签名头文件内容。若校验通过，则获取签名头文件文件摘要并存储在非易失性存储器中。Bootloader 获取 Ecu 中整个 App 数据，并通过对称加密 SHA256 算法，计算得出 Hash Value。

When the Bootloader performs the flashing process, it uses the asymmetric encryption algorithm and the root public key to verify the content of the signature header file. If the verification is successful, it retrieves the file summary from the signature header and stores it in

non-volatile memory. The Bootloader then obtains the entire App data from the ECU and calculates the Hash Value using the symmetric encryption SHA256 algorithm.

对比 Hash Value 和存储在非易失性存储器中的文件摘要，实现知从青龙 Bootloader 安全刷写功能。

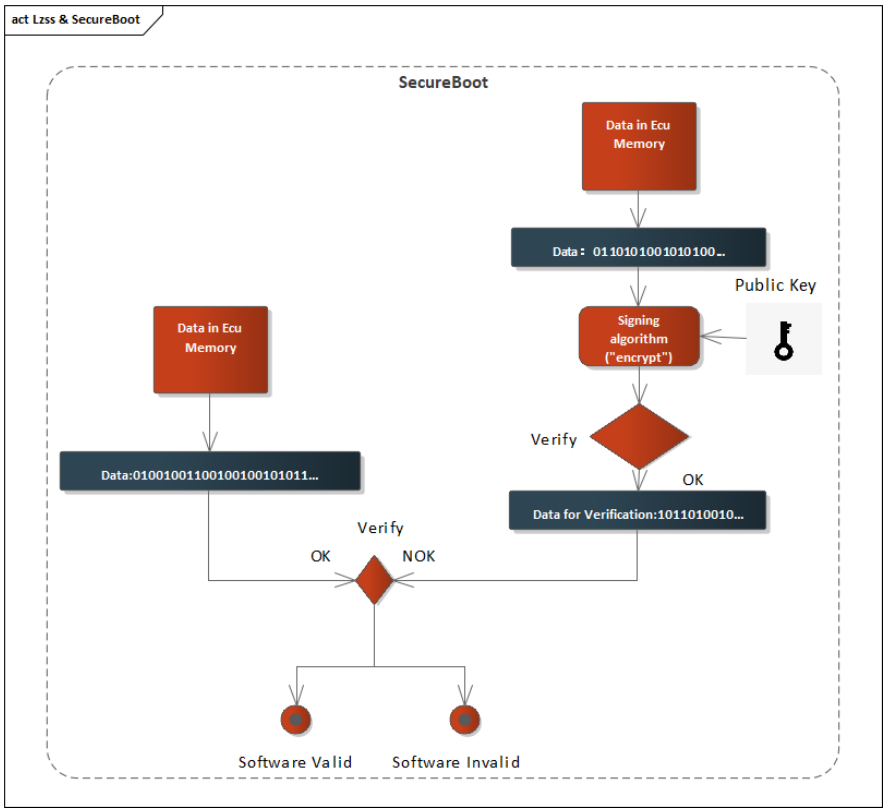
Compare the Hash Value with the file summary stored in non-volatile memory to implement the secure flashing feature of the ZC.QingLong Bootloader.

- 安全启动功能：

  Secure Boot Feature

知从青龙 BootLoader 支持 SMTC 规范的 SecureBoot 流程中的安全启动功能，下图为简化示例图：

ZC.QinLong Supports the Secure Boot process according to the SMTC specifications, which includes the secure boot feature. Below is a simplified example diagram:



当 Bootloader 执行上电启动或执行复位启动时，Bootloader 获取存储在 Ecu Memory 中的数据，通过非对称加密算法和公钥对数据进行解密验签。当验签成功则获取 Verification Data，并与存储在非易失性存储器中的文件摘要进行对比。若对比成功则可以实现安全启动功能。

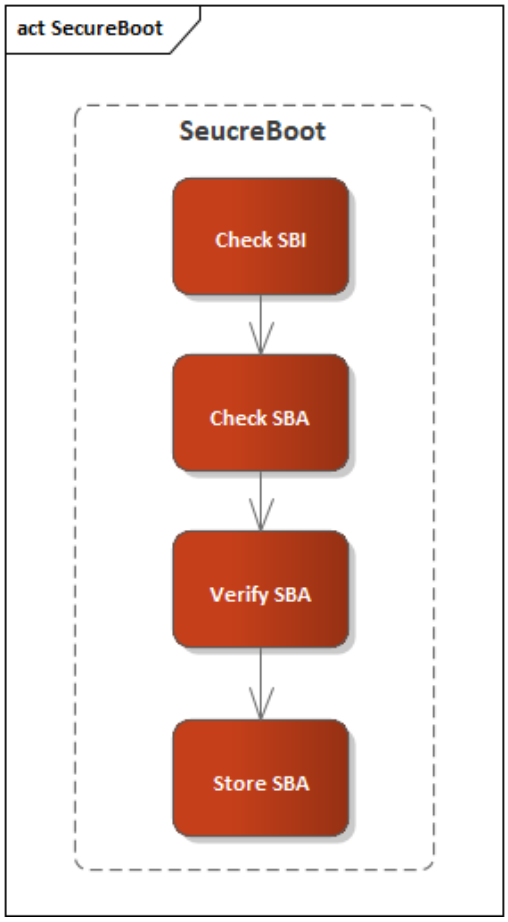
When the Bootloader performs a power-on startup or a reset startup, it retrieves data stored in the ECU memory. It then uses the asymmetric encryption algorithm and a public key to decrypt and verify the signature of the data. If the verification is successful, the Bootloader obtains the Verification Data and compares it with the file summary stored in non-volatile memory. If the comparison is successful, the secure boot function can be realized.

- 签名旁路功能：

  Signature Bypass Feature

知从青龙 BootLoader 支持 SMTC 规范的 SecureBoot 流程中的签名旁路验证功能，下图为简化示例图：

ZC.QinLong BootLoader Supports the signature bypass verification feature in the SecureBoot process according to the SMTC specifications. Below is a simplified example diagram



当 Bootloader 执行上电启动或执行复位启动时，Bootloader 会检测 SBI 旁路签名标志位是否置起，当 SBI 置起时将会开始检测签名旁路许可证 SBA 是否写入。

During power-on or reset startup, the Bootloader checks if the Signature Bypass Indicator (SBI) flag is set. If the SBI is set, the Bootloader will then proceed to check whether the Signature Bypass Authority (SBA) license has been written.

如果签名旁路许可证 SBA 已写入，则 Bootloader 将会检测 SBA 中的签名与 Application 的签名是否一致。

If the Signature Bypass Authority (SBA) license has been written, the Bootloader will then check if the signature in the SBA matches the signature of the Application.

当 SBA 验证成功后，将会保存 SBA 有效标志位，在后续的安全启动流程中，若 SBA 有效位被置起，安全启动以及安全刷写流程中的签名刷新文件授权性和完整性校验将不需要执行。

When the SBA (Signature Bypass Authority) verification is successful, the SBA valid flag will be saved. In the subsequent secure boot process, if the SBA valid flag is set, the signature refresh file's authorization and integrity checks in the secure boot and secure flashing processes will not be required.

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	ZC 对软件的需求分析 ZC's Software 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	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

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

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

公众号 业务联系
成为全球领先的汽车基础软件公司
To Be the Global Leading Automotive Basic Software Company