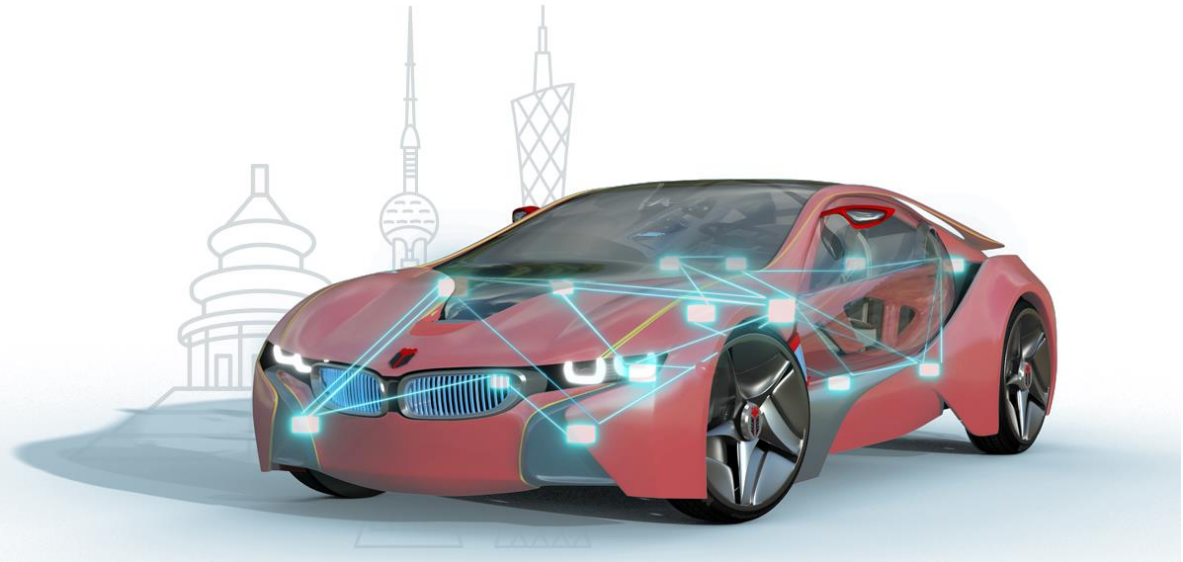
知从青龙云途 YTM32B1HA0X 安全启动介绍

ZC.QINGLONG YUNTU YTM32B1HA0X SECUREBOOT INTRODUCTION

知从青龙 BootLoader

ZC.QingLong BootLoader



知从青龙云途 YTM32B1HA0X 安全启动介绍

ZC.QINGLONG YUNTU YTM32B1HA0X SECUREBOOT INTRODUCTION

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 refreshing software (BootLoader) by ZC. Controllers using ZC.QingLong BootLoader can achieve the update function of the application program through communication methods such as CAN, LIN, SPI, and UART. ZC.QingLong BootLoader supports chips from NXP, Infineon, Renesas, ST, and other manufacturers, and also supports the program refreshing standards of many car manufacturers, offering customized development services.

知从青龙 SecureBoot 支持基于 YunTu YTM32B1HA0x 平台实现 SecureBoot 功能。控制器可以通过 SecureBoot 功能在启动阶段检测 BootLoader 软件和 Application 软件的代码数据是否被篡改，保证汽车软件运行的安全性。

The ZC.QingLong SecureBoot supports the implementation of SecureBoot functionality based on the YunTu YTM32B1HA0x platform. The controller can utilize the SecureBoot feature during the boot phase to verify whether the code data of the BootLoader software and Application software has been tampered with, ensuring the security of automotive software operations.

2 应用领域 APPLICATION FIELD

知从青龙 SecureBoot 软件可应用于使用 YTM32B1HA0x 系列芯片的控制器应用程序编程功能。支持的控制器包括:

The SecureBoot software from ZhiCong Qinglong can be applied to controller application programming functions utilizing the YTM32B1HA0x series chip. The supported controllers include:

- 动力总成与底盘 Powertrain and Chassis
  - 整车控制器 VCU
  - 电池管理系统 BMS
  - 电动助力转向 EPS
  - 防抱死系统 ABS
  - 电控行驶稳定系统 ESP
  - 电子制动力分配 EBD
  - 线控刹车系统 EPB
  - 驱动防滑系统 ASR
  - 尾气回收处理 EGR
- 车身控制与网关 Body Control and Gateway
  - 车身域控制器 BDC
  - 入门级区域控制器 Entry-Level ZCU
- 智能座舱与显示 Smart Cockpit and Display
  - 智能座舱辅助 MCU
  - 抬头显示 AR-HUD
  - 智能矩阵大灯 ADB

3 配置环境 CONFIGURATION ENVIRONMENT

配置环境 Configuration Environment	
Hardware (Chip)	YTM32B1HA0x
Compilers Supported	IAR Arm 9.40.1
Debugger	Isystem (IC5000 / IC5700)

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 trends of electrification, intelligence, connectivity, and sharing in the automotive industry, 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, the capability to update software is required at each stage. Therefore, the demand from customers for software program updates is becoming more urgent.

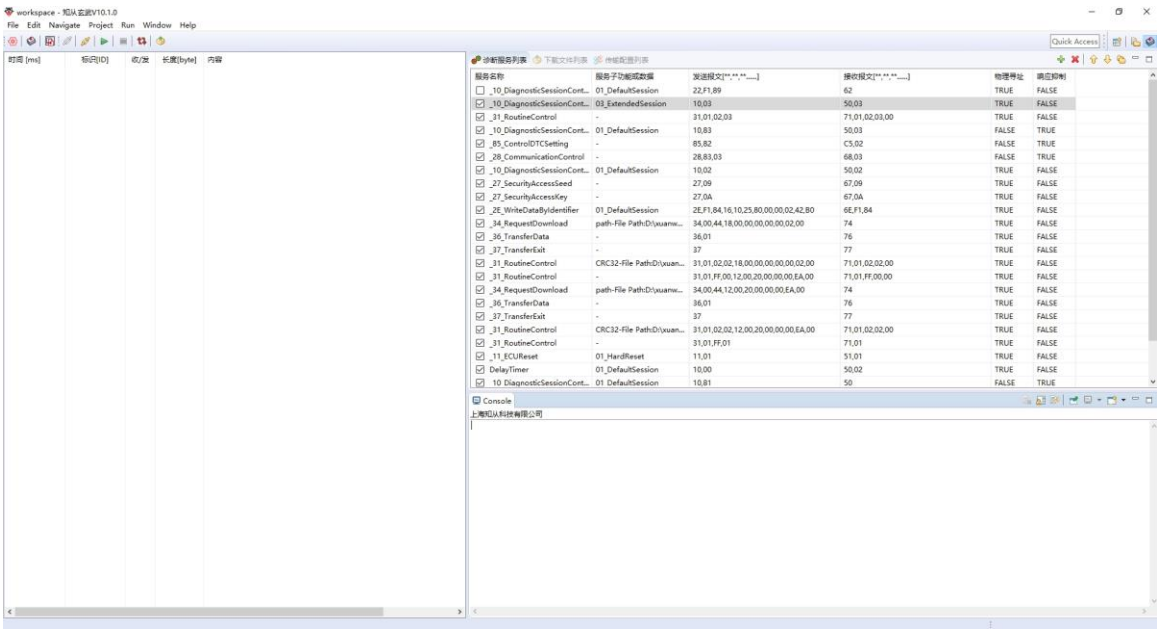
并且，随着车联网的落地，信息安全越来越受重视，芯片作为信息的载体，因此，对芯片中的数据保护尤其重要。知从青龙 SecureBoot 基于 YunTu YTM32B1HA0x 平台，实现 BootLoader 的 Security 功能。通过实现 SecureBoot，控制器可以识别 BootLoader 程序和应用程序是否被篡改，特别是在 Application 更新过程中，可以保证程序刷新的安全性。

Furthermore, with the implementation of the Internet of Vehicles, information security is gaining more attention. As chips serve as carriers of information, the protection of data within the chips is particularly important. ZC.QingLong SecureBoot, based on the YunTu YTM32B1HA0x platform, implements the security features of the BootLoader. By implementing SecureBoot, the controller can detect whether the BootLoader program and application program have been tampered with, especially during the updating applicaiton process, ensuring the security of the program update.

5 功能描述 FUNCTIONAL DESCRIPTION

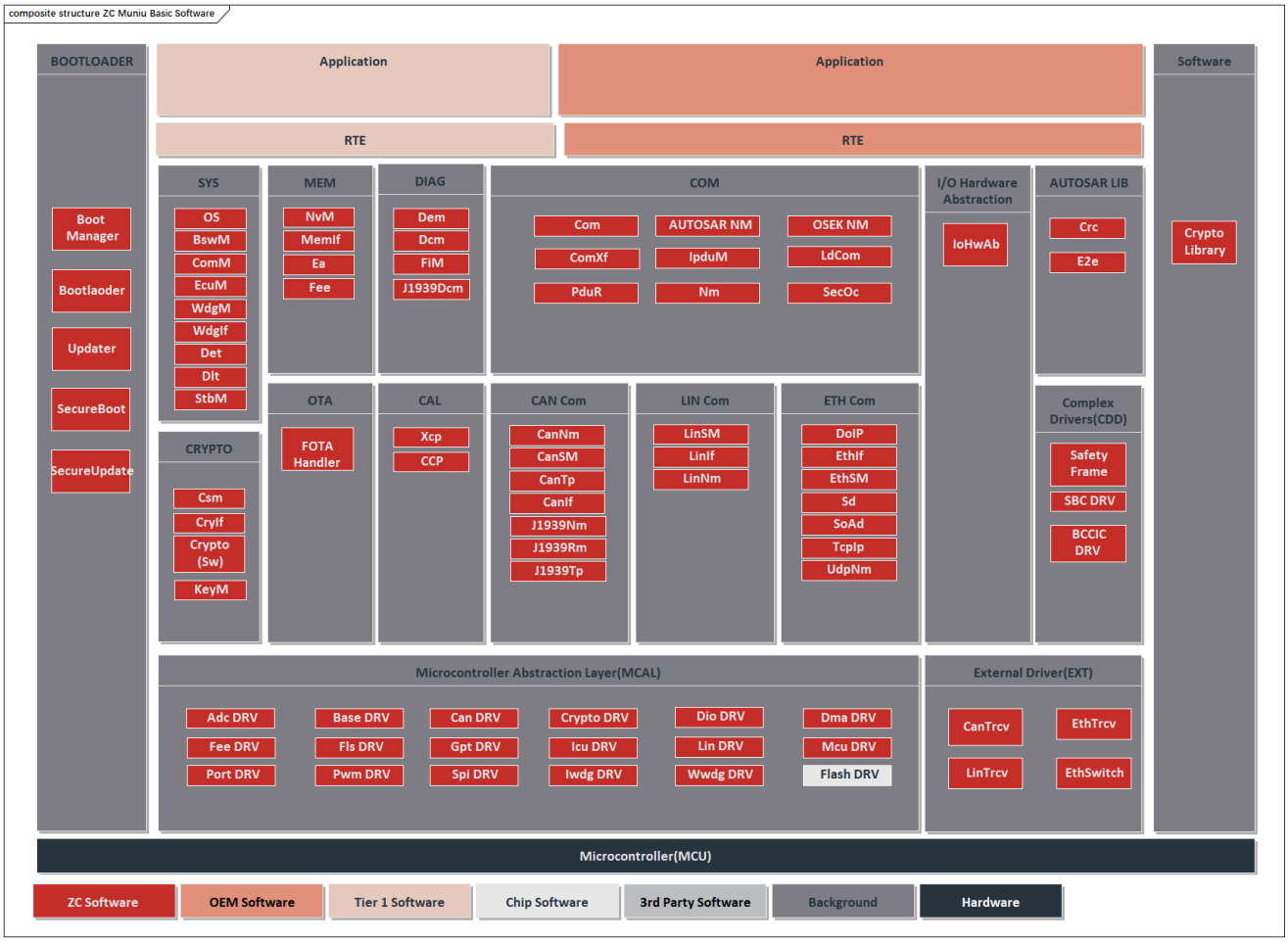
5.1 产品特点 Product Features

- 适用于多达十几家整车厂的程序更新规范
  Suitable for the program update specifications of up to a dozen car 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
  Supports self-update functionality for BootLoader
- 支持 HIS 规范
  Supports HIS specifications
- 支持 CAN/LIN/SPI/UART 等通信
  Supports communication via CAN/LIN/SPI/UART, etc.
- 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, offering a complete solution for program updates
- 支持对称加密 SHA256 和 AES128 算法
  Supports symmetric encryption algorithms SHA256 and AES128
- 支持非对称加密 ECC 和 RSA 算法
  Supports asymmetric encryption algorithms ECC and RSA



知从玄武—程序更新工具
ZC.XuanWu—Software 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 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：

The Qinglong 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

  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。

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

  Can 模块支持 CAN、CANFD 通信功能。

  The Can module supports CAN and CANFD communication functions.

- 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。

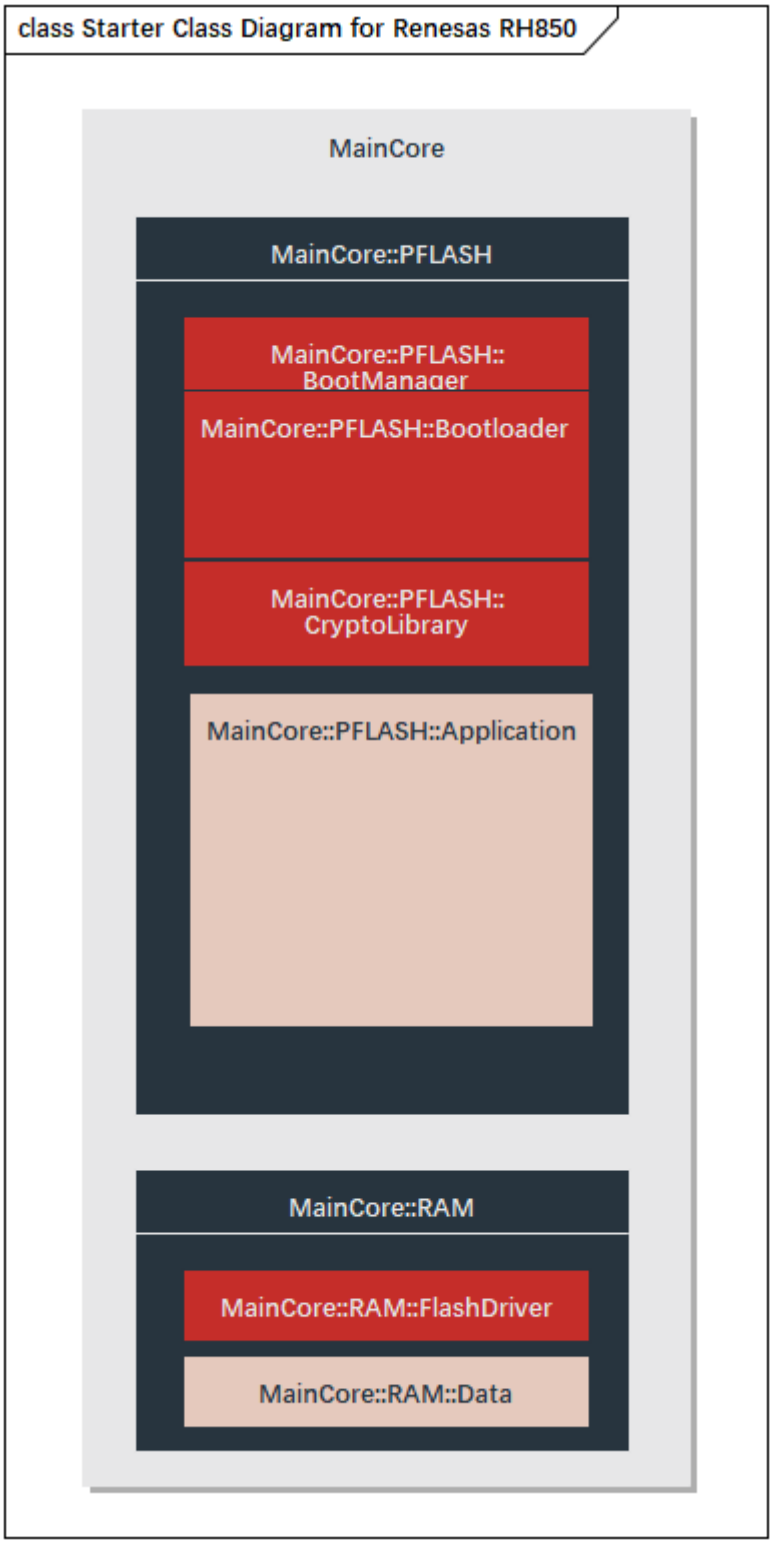
  The Dcm module realizes the diagnostic function based on the support of the communication module, meeting the definitions of ISO 14229 and ISO 15765 standards.

- Crypto

  SecureBoot 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 YunTu 芯片内置加密库提高信息安全功能的稳定性和校验速度。

  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 YunTu chip with built-in crypto library to improve the stability and verification speed of the Cybersecurity function.

5.3 内存结构 Memory Structure



云途芯片的内存分为 PFLASH 和 RAM，PFLASH 区分为 Application&Data、BootManager 和 BootLoader 区，RAM 区分为 FLASH Driver 和 Data。

Crypto Library 存储于 PFlash 中，在软件运行过程中被 BootManager 和 Bootloader 调用。

The memory of the YunTu chip comprises PFLASH and RAM. The PFLASH section is divided into Application & Data, BootManager, and Bootloader areas, while the RAM section is divided into FLASH Driver and Data.

The Crypto Library is stored within PFLASH and is invoked by the BootManager and Bootoader during software execution.

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

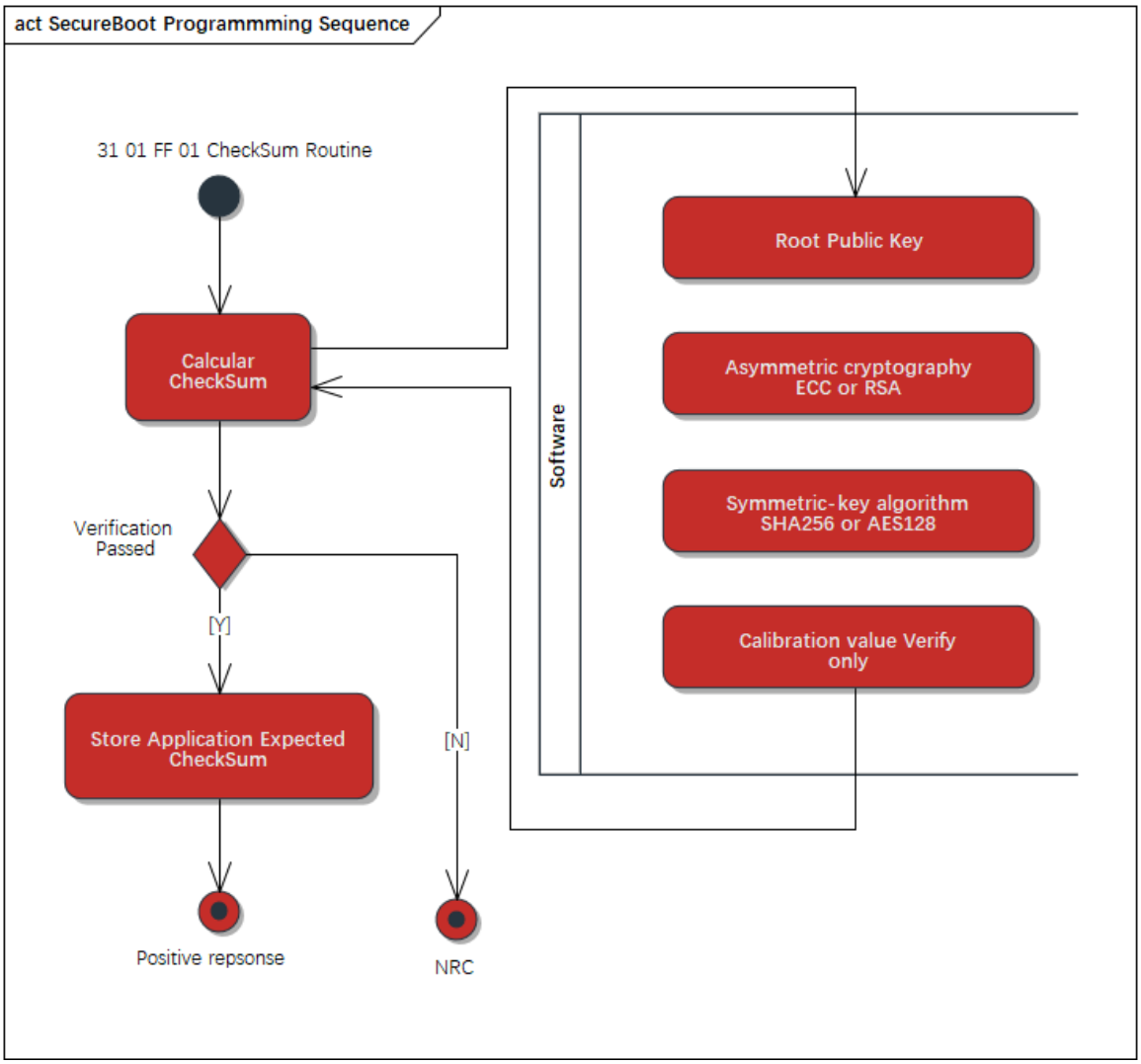
知从青龙 SecureBoot 支持安全刷写与安全启动功能。

ZC.QingLong SecureBoot supports the functions of secure flashing and secure booting

- 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，通过调用 SecureBoot 中的非对称加密算法 ECC 或 RSA 接口，对数据进行真实性校验。若校验成功则通过对称加密算法 SHA256 或 AES128 对数据完整性进行校验，保证安全刷写流程。

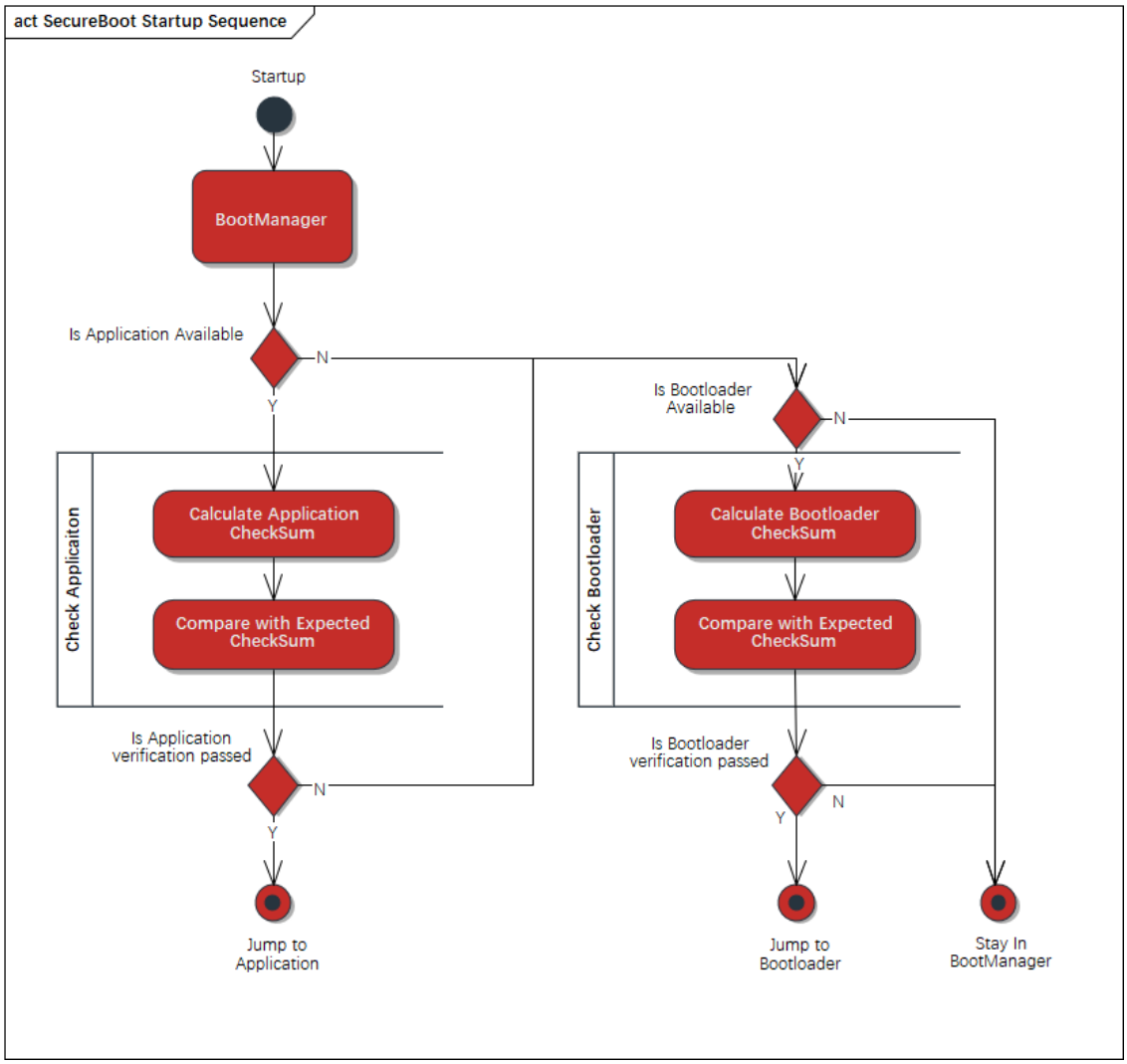
ZC.QingLong SecureBoot performs data authenticity verification by invoking the asymmetric encryption algorithms ECC or RSA interfaces within the SecureBoot, based on the Root Public Key stored in non-volatile memory. If the verification is successful, it then checks the integrity of the data through symmetric encryption algorithms like SHA256 or AES128, ensuring the secure flashing process.



- 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。

During the process from power-on to jumping into the Application, ZC.QingLong SecureBoot supports the secure boot function. It verifies the security of the Boot and Application programs through symmetric encryption algorithms like SHA256 or AES128, ensuring the program starts securely.



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	客户需求文档 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
	集成手册 Integration Manual

开发流程 Development Process	文档描述 Document Description
Software Integration and Integration Testing	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14035707号

软件名称：知从青龙BootLoader软件
[简称：知从青龙]
V9.1.0

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：2024SR1631834

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

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