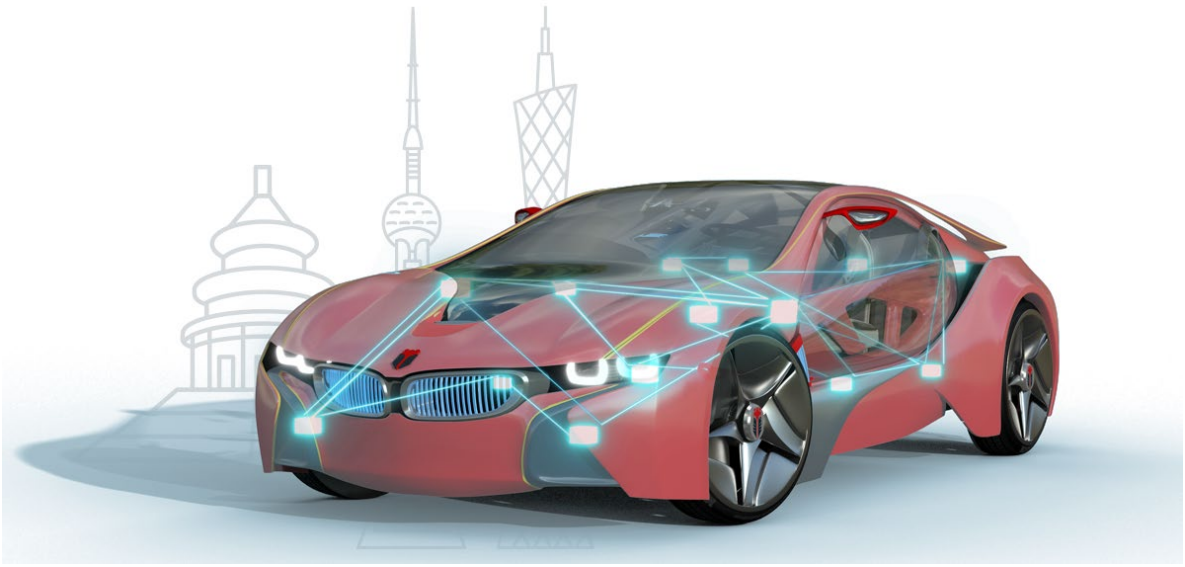
知从青龙 SECUREBOOT 恩智浦 S32K3
CHERY QSQR 产品手册
ZC.QINGLONG SECUREBOOT PRODUCT MANUAL
BASED ON NXP S32K3 FOR CHERY QSQR

知从青龙 BootLoader

ZC.QINGLONG BootLoader



知从青龙 SECUREBOOT 恩智浦 S32K3
CHERY QSQR 产品手册
ZC.QINGLONG SECUREBOOT PRODUCT MANUAL
BASED ON NXP S32K3 FOR CHERY QSQR

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 application programs through communication methods such as CAN, LIN, SPI, and UART. Currently, ZC.QingLong BootLoader supports chips from NXP, Infineon, Renesas, ST, and other manufacturers, and also supports the program refreshing standards of various car manufacturers, offering customized development services.

知从青龙 SecureBoot 基于 NXP S32K3 平台，实现对 QSQR 规范 Security 功能的支持。目前知从青龙 SecureBoot 已实现支持 CBF 文件刷写、AB 区划分功能、多组 RSA 和 SHA 组合算法解析、签名认证等功能需求，满足 QSQR 规范中大部分的刷写需求。

ZC Qinglong SecureBoot, based on the NXP S32K3 platform, implements support for QSQR specification security features. Currently, ZC.Qinglong SecureBoot has realized support for CBF file flashing, AB partitioning, parsing of multiple RSA and SHA combination algorithms, signature authentication, and other functional requirements, meeting most of the flashing needs specified in QSQR.

CHERY

支持 QSQR
电子电气架构

2 应用领域 APPLICATION FIELDS

知从青龙 SecureBoot 可应用于使用 S32K3 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 refreshing functions that use the S32K3 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)	S32K312
Compilers Supported	GreenHills v2021.1 S32DS_ARM_v3.4
Debugger	Lauterbach (Trace32 R.2021.02) Isystem (IC5700)

GreenHills 编译器 GreenHills Compiler	
编译选项 Compilation options	-cpu=cortexm7 -DS32K312 -thumb -fsingle -DGHS -DAUTOSAR_OS_NOT_USED -DS32K312 -DUSE_SW_VECTOR_MODE -C99 -Osize -Wall-G -c --unsigned_fields --unsigned_chars -keeptempfiles -preprocess_assembly_files --no_exceptions -dual_debug --prototype_errors -Wundef -noslashcomment -Wimplicit-int -Wshadow -Wtrigraphs -nostartfile --no_commons --incorrect_pragma_warnings -list --short_enum --ghstd=last --gnu_asm
链接选项 Linking options	-e Reset_Handler -map -keepmap -Mn -delete -ignore_debug_references -L thumb2 -lmath_sd -larch -lstartup -lind_sd -keep=C40_Ip_AccessCode

S32DS 编译器 S32DS Compiler	
编译选项 Compilation Options	-O0 -g3 -Wall -c -fno-short-enums -ffunction-sections -fdata-sections -Wstrict-prototypes -Wsign-compare -Werror=implicit-function-declaration -Wundef -Wdouble-promotion -mcpu=cortex-m7 -mthumb -mlittle-endian -mfloat-abi=hard -mfpu=fpv5-sp-d16 -specs=nano.specs -specs=nosys.specs
链接选项 Linking Options	-nostartfiles --entry=Reset_Handler -ggdb3 -T "linker_flash_s32k312.ld" -Wl,-Map,"S32K312_Bootloader.map" -mcpu=cortex-m7 -mthumb -mlittle-endian -mfloat-abi=hard -mfpu=fpv5-sp-d16 -specs=nano.specs -specs=nosys.specs

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 automobiles is becoming increasingly complex. With the electrification, intelligence, connectivity, and sharing of vehicles, the proportion of software R&D in automobiles is growing larger. The frequency of software updates is also increasing. Moreover, throughout the entire lifecycle of a car, including the R&D phase, production phase, and after-sales phase, software update functionality is required in each stage. Therefore, customer demand 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 NXP S32K1xx 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。

Furthermore, with the implementation of the Internet of Vehicles, information security is gaining more attention. As chips serve as carriers of information, data protection within the chips is particularly important. ZC.Qinglong SecureBoot, based on the NXP S32K1xx platform, implements the security features of the BootLoader. By implementing SecureBoot, the controller can detect if the BootLoader program and application programs have been tampered with, ensuring the security of program updates, especially during the FOTA process.

QSQR 电子电气架构在 SecureBoot 中，通过实现 AB 分区切换、Secure Boot、CBF 加密签名验证等功能，降低了在 MCU 更新过程中的安全风险，大幅提升了 SecureBoot 的安全性以及可靠性。

The QSQR electronic and electrical architecture in SecureBoot, by implementing features such as AB partition switching, Secure Boot, and CBF encryption signature verification, reduces security risks during the MCU update process and significantly enhances the security and reliability of SecureBoot.

5 功能描述 FUNCTIONAL DESCRIPTION

5.1 产品特点 Product Feature

- 适用于 QSQR 平台规范

  Suitable for QSQR platform specifications

- 支持 AB 分区切换等功能

  Supports features such as AB partition switching

- 支持应用程序和数据的更新功能

  Supports update functions for applications and data

- 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

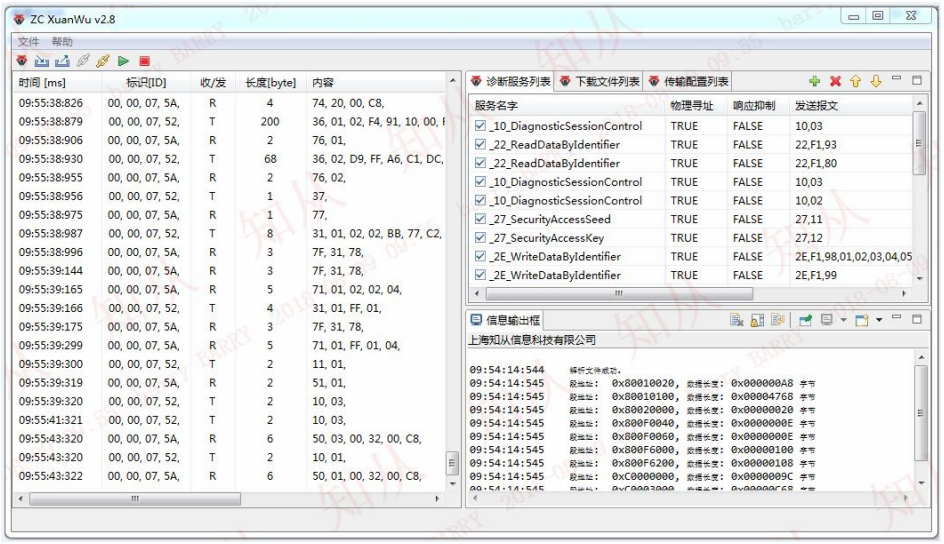
  Adapts to ZhiCong Xuanwu program update tools, offering a complete solution for program updates

- 支持多种 RSA 和 SHA 规范的组合算法

  Supports various combinations of RSA and SHA standard algorithms

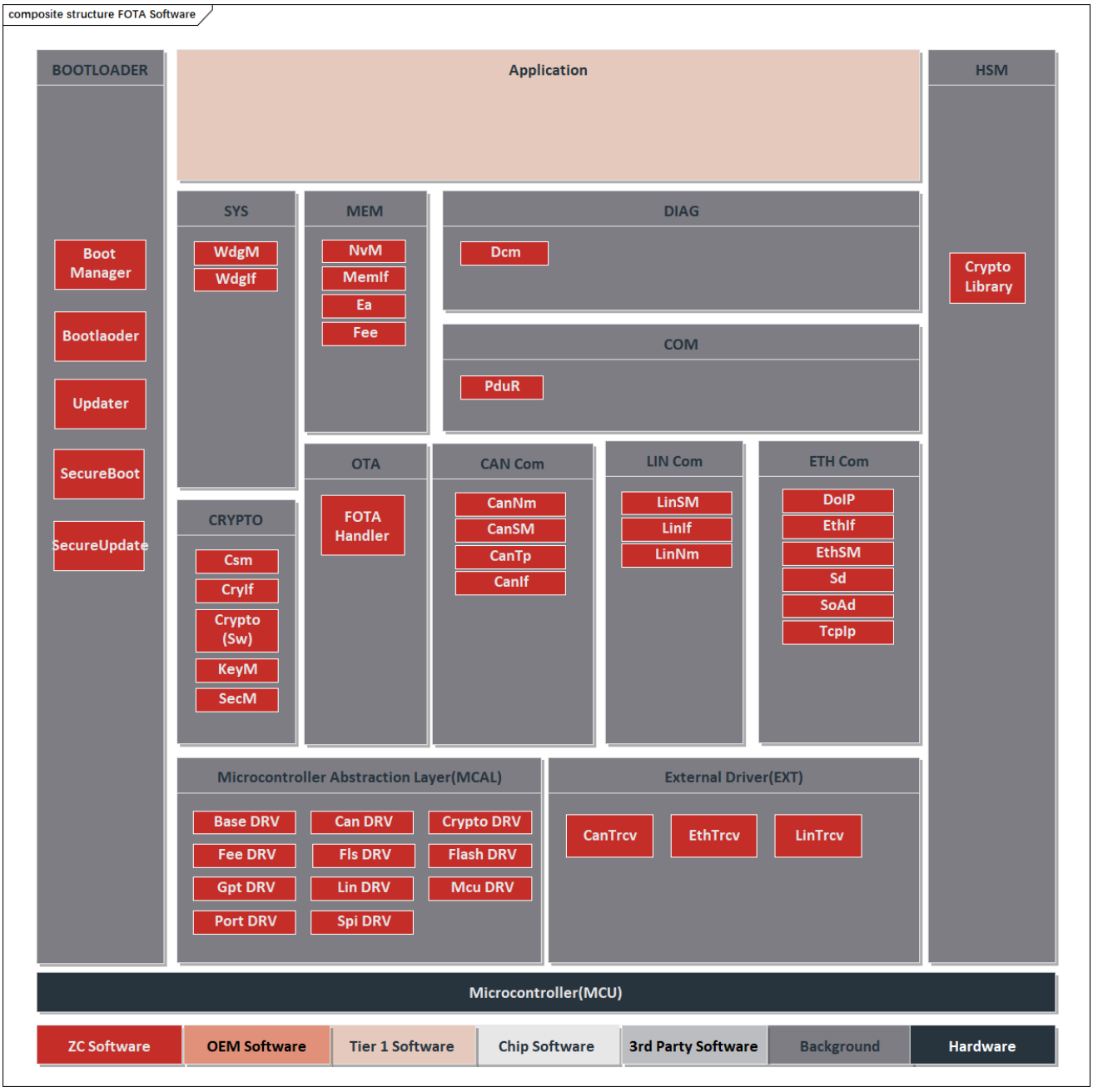
- 支持 CBF 文件解析

  Supports CBF file parsing



知从玄武—程序更新工具
ZC.XUNWU—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.

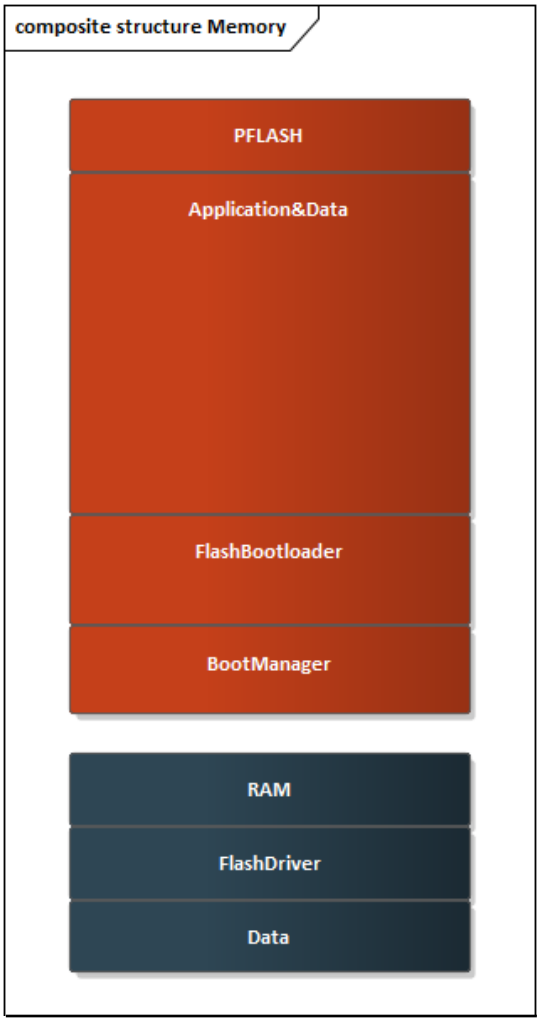
- Dcm

  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、FlashBootloader 和 BootManager 区，RAM 区分为 FlashDriver 和 Data。

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

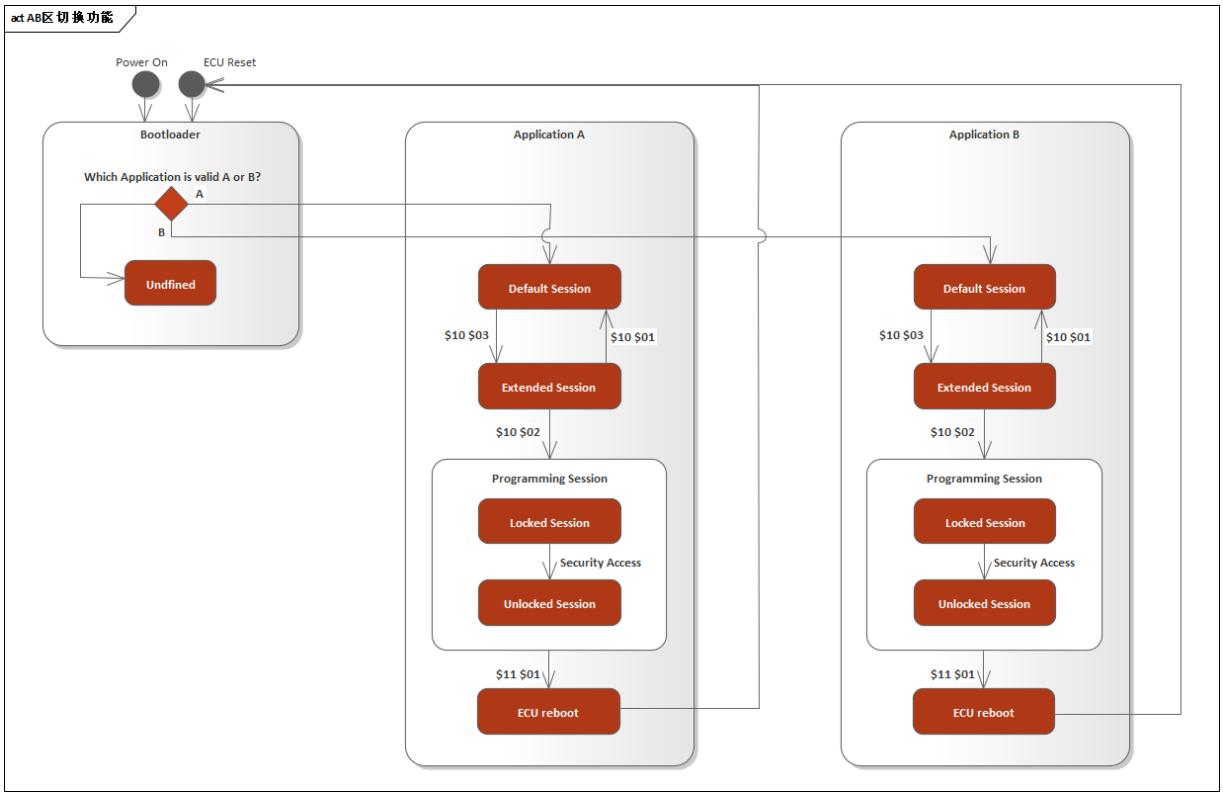
5.4 支持 QSQR 规范 Supports QSQR specifications

知从青龙 SecureBoot 支持 QSQR 规范的刷写流程和功能需求，以下为部分已实现的 QSQR 规范的需求功能：

ZC Qinglong SecureBoot supports the flashing process and functional requirements of the QSQR specifications. The following are some of the QSQR specification requirements that have been implemented:

- AB 分区：

AB Partitioning:



知从青龙 SecureBoot 支持 AB 分区功能。SecureBoot 会根据 AB 区有效标志位判断跳转更新后的 Application，用户可以通过相关指令操作执行 AB 区切换功能，例如回滚、备份等功能。

ZC Qinglong SecureBoot supports the AB partition feature. SecureBoot determines which Application to jump to after updating based on the active flag of the AB partitions. Users can perform AB partition switching functions such as rollback and backup through related command operations.

- 加密算法：

  Encryption Algorithms:

知从青龙 SecureBoot 支持通过多种 RSA 和 SHA 组合算法执行完整性校验，例如 SHA1、SHA256 、 SHA512 、 RSA1024+RSASS-PKCS1-V1_5 、 RSA2048+ RSASS-PKCS1-V1_5 、RSA4096+RSASSA-PSS 等算法。

ZC Qinglong SecureBoot supports integrity checks through various combinations of RSA and SHA algorithms, such as SHA1, SHA256, SHA512, RSA1024+RSASS-PKCS1-V1_5, RSA2048+RSASS-PKCS1-V1_5, RSA4096+RSASSA-PSS, and other algorithms.

- 支持 CBF 文件下载：
  Support for CBF File Download:

通过搭配知从玄武程序更新工具，知从青龙 SecureBoot 可以解析 CCBF 文件数据，将数据下载到 ECU 中，并按照 QSQR 规范使用 CBF 中携带的 Verification Block 和 Signature 数据对完整性和可靠性进行校验。

By integrating with the ZC.Xuanwu program update tool, ZC.Qinglong SecureBoot can parse CCBF file data, download the data into the ECU, and verify the integrity and reliability according to the QSQR specifications using the Verification Block and Signature data carried in the CBF.

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
	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	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 廿五 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