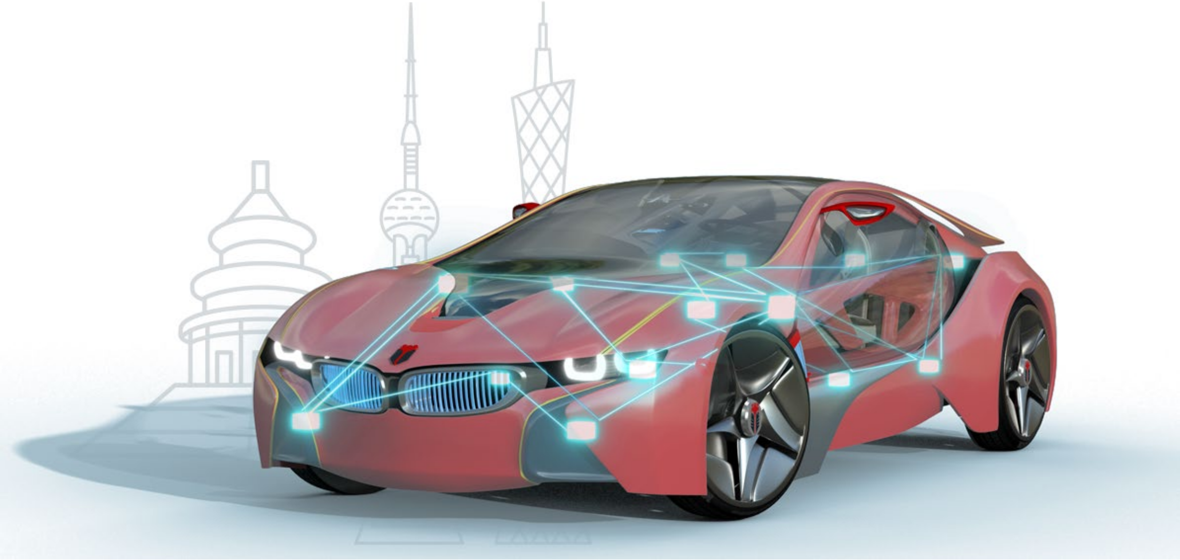
知从青龙 FOTA 方案手册

ZC.QINGLONG FOTA SOLUTION MANUAL

知从青龙 FOTA 平台

ZC.QingLong FOTA platform



知从木牛 FOTA 方案手册

ZC.QINGLONG FOTA SOLUTION MANUAL

知从青龙 FOTA 平台

ZC.QingLong FOTA platform

1　方案介绍 SOLUTION INTRODUCTION

早期的汽车电子主要以硬件为主，然而随着汽车电子软件的不断发展， FOTA 正在占据重要的位置。随着汽车软件的不断更新迭代，汽车电子 FOTA 功能的需求也日益增多。

In the early days, automotive electronics were primarily hardware-centric. However, with the ongoing development of automotive electronic software, FOTA is taking on a significant role. As automotive software continues to be updated and iterated, the demand for FOTA features in automotive electronics is also increasing.

MCU 端的 FOTA 是汽车电子 OTA 更新环节中的重要一环:

The FOTA on the MCU side is a vital component of the automotive electronics OTA update process:

- 安全启动（SecureBoot）可以有效防止攻击者恶意修改软件;
  Secure Boot effectively prevents attackers from maliciously modifying the software.
- 升级软件（Updater）可以更新 Bootloader 软件，确保 Boot 符合最新的刷写流程;
  Updater can update the Bootloader software, ensuring that the Boot process aligns with the latest flashing procedures.
- 无线升级（FOTA）可以在汽车运行过程中执行远程无线升级，配合 AB 分区、差分刷写等功能，可以高效地升级固件功能。
  Wireless updates (FOTA) can execute remote wireless upgrades during the vehicle's operation, and when combined with features like AB partitioning and differential flashing, it can efficiently upgrade firmware capabilities.

2　安全启动 SECUREBOOT

知从科技可以为客户提供 SecureBoot 完整方案，并可针对项目特定需求和硬件模块定制开发：

ZC can provide customers with a complete SecureBoot solution and can customize the development according to specific project requirements and hardware modules：

- 基于硬件加密方案

  Hardware-based encryption solution
- 基于软件加密方案

  Software-based encryption solution
- 密钥存储管理方案

  Key storage management solution
- 安全启动失效分析

  Secure Boot failure analysis
- 产线生产模式方案

  Production line production mode solution
- 数据压缩下载

  Data compression download
- 数据加密升级

  Data encryption upgrade

安全启动（SecureBoot）是 MCU 的基本功能，通过硬件加密模块来实现，该机制必须独立于用户程序运行，不能被破坏。作为整个安全启动信任链的基础，安全启动主要用于在 MCU 启动之后，用户程序执行之前，对用户定义的 Flash 中关键程序的数据完整性和真实性进行验证，确定是否被篡改。如果验证失败，说明 MCU 处于不可信的状态，部分功能甚至整个程序不能运行。

Secure Boot is a fundamental feature of the MCU, implemented through hardware encryption modules. This mechanism must operate independently of the user program and cannot be compromised. As the foundation of the entire secure boot trust chain, Secure Boot is primarily used to verify the integrity and authenticity of key programs in the user-defined Flash after the MCU starts and before the user program is executed, to ensure they have not been tampered with. If the verification fails, it indicates that the MCU is in an untrusted state, and some functions or even the entire program cannot be executed.

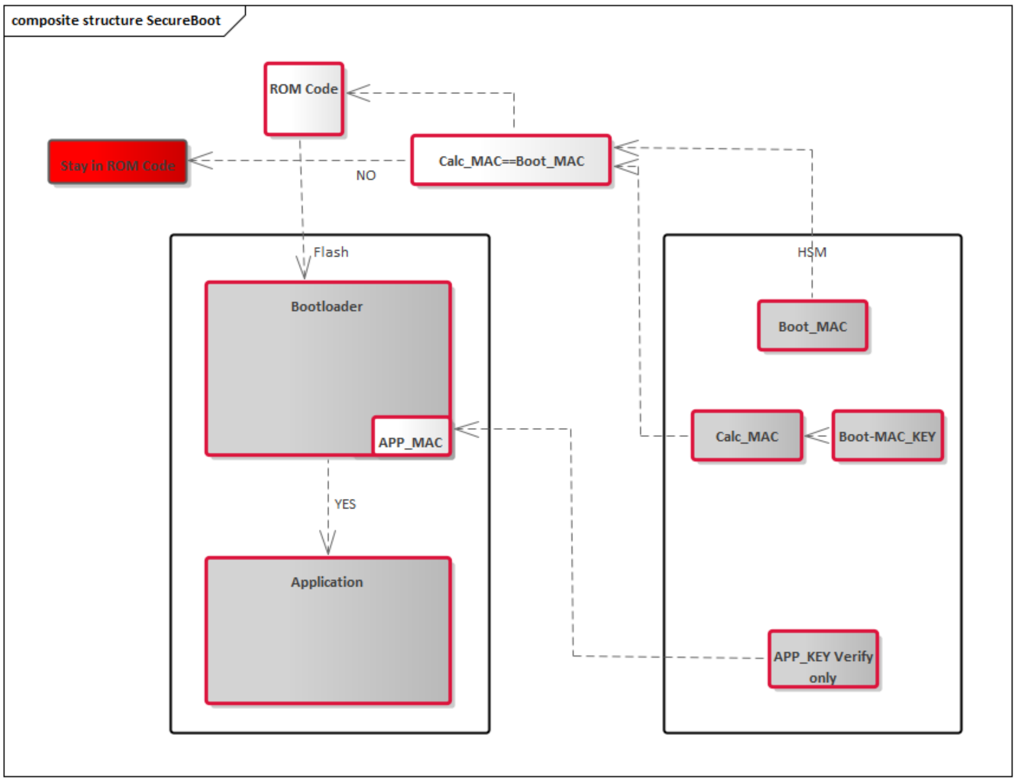


FIGURE 2 Secure Boot

- 安全启动信任根 Secure Boot Trust Root

  安全启动依赖于芯片硬件支持，用于提供初始信任根的可执行代码和密钥。 信任根密钥用于信任根代码验证已签名软件或已签名的软件关键数据部分内容的第一个启动阶段。此签名软件用于验证软件组件的后续运行阶段代码。 密钥应该由 OEM 在生产阶段供应给硬件厂商， 并存储在受保护内存中。

  Secure Boot relies on the hardware support of the chip to provide the initial trust root with executable code and keys. The trust root key is used by the trust root code to verify the first boot phase of the signed software or the content of the key data part of the signed software. This signed software is used to verify the code of subsequent operational phase software components. The key should be supplied by the OEM to the hardware manufacturer during the production phase and stored in protected memory.

- 安全启动信任链 Secure Boot Trust Chain

  安全启动信任链是由信任根代码建立的。通过信任根代码的 root 对第一阶段引导程序进行验证，验证成功则可通过此验证有效的软件执行并继续验证后续引导阶段软件有效性。

  The Secure Boot Trust Chain is established by the trust root code. The root of the trust root code verifies the first stage of the boot loader. If the verification is successful, the verified software can be executed and the validity of the subsequent boot phase software can continue to be verified.

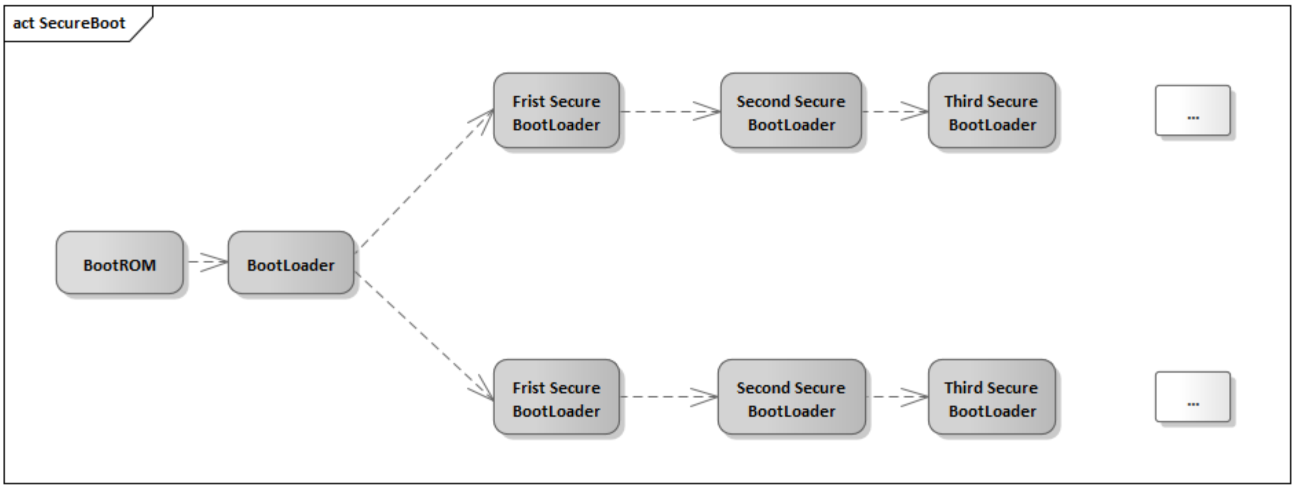


图 3 Secure Boot Routine

- 安全启动过程 Secure Boot process

通过数据内容加密可实现对数据的保护以防止数据被泄露，同时也可防止数据在传输过程中被篡改。加密算法一般分为对称加密算法和非对称加密算法。对称加密算法的加密和解密使用相同密钥，而非对称算法则使用公钥和私钥加解密数据内容。公钥私钥成对存在，例如用公钥加密需用私钥解密，反之亦然。

Encrypting data content can protect data from being disclosed and also prevent data from being tampered with during transmission. Encryption algorithms are generally divided into symmetric encryption algorithms and asymmetric encryption algorithms. Symmetric encryption algorithms use the same key for both encryption and decryption, while asymmetric algorithms use a public key for encryption and a private key for decryption. The public and private keys exist in pairs; for example, data encrypted with the public key must be decrypted with the private key, and vice versa.

AES 是最常用的对称加密算法，其拥有运算速度快，内存需求低，分组长度和密钥长度设计灵活等优点。对于非对称加密算法来说，典型的有 RSA 和 ECC 两种加密算法。RSA 加密算法常被选择用于镜像的签名与验签。

AES is the most commonly used symmetric encryption algorithm, known for its fast computation speed, low memory requirements, and flexible block and key length design. For asymmetric encryption algorithms, typical examples include RSA and ECC. The RSA encryption algorithm is often chosen for signing and verifying images.

知从科技所开发的青龙 SecureBoot 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 以及国密算法等。

The QingLong SecureBoot developed by ZC includes the core firmware of the hardware security module (zHSM CORE) and the customer application interface functions (SHE CD). In addition to meeting the conventional SHE functions (key injection, symmetric encryption and decryption, message authentication code generation and verification, random number generation, and secure boot, etc.), the core firmware can also be extended to support various algorithms, such as HASH, ECC256, and national cryptographic algorithms.

3 升级软件 UPDATER

知从科技可以为客户提供 Updater 完整方案，并可针对项目特定需求和硬件模块定制开发：

ZC can provide customers with a complete Updater solution and can customize development according to specific project requirements and hardware modules:

- 更新版本校验功能 Version verification function

升级软件（Updater）是汽车电子软件升级迭代的重要手段，主要用于将 Bootloader 的刷写流程进行更新，符合 OEM 最新的刷写流程方案。汽车电子软件在开发和使用过程中，由于硬件的限制以及软件部分模块功能的缺失，通常在首次发售时仅满足初版的 OEM 刷写规范。在后续应用软件更新的情况，为了使 Bootloader 软件也同步适配最新的 OEM 刷写规范以及修复 Bootloader 中存在的 Bug，可以通过 Updater 软件更新 Bootloader 功能，减少软件升级的工作量并提高软件升级的效率。

The Updater is an important means for the upgrade and iteration of automotive electronic software, mainly used to update the flashing process of the Bootloader to comply with the latest flashing process scheme of the OEM. During the development and use of automotive electronic software, due to hardware limitations and the lack of some software module functions, it usually only meets the initial version of the OEM flashing specifications when first released. In the case of subsequent application software updates, in order to synchronize the adaptation of the Bootloader software to the latest OEM flashing specifications and to fix bugs in the Bootloader, the Bootloader function can be updated through the Updater software, reducing the workload of software upgrades and improving the efficiency of software upgrades.

知从科技所开发的青龙 Bootloader 支持 Updater 的版本校验、升级等功能。可以实现不同 OEM 的规范要求，可定制开发等。Updater 在软件更新中起到重要的作用，它可以确保 Bootloader 在使用过程中也可以像应用软件一样进行更新迭代。

The Qinglong Bootloader developed by ZC supports Updater's version verification, upgrade, and other functions. It can meet the specification requirements of different OEMs and can be customized for development. The Updater plays an important role in software updates, ensuring that the Bootloader can also be updated and iterated like the application software during its use.

4 无线升级 FOTA

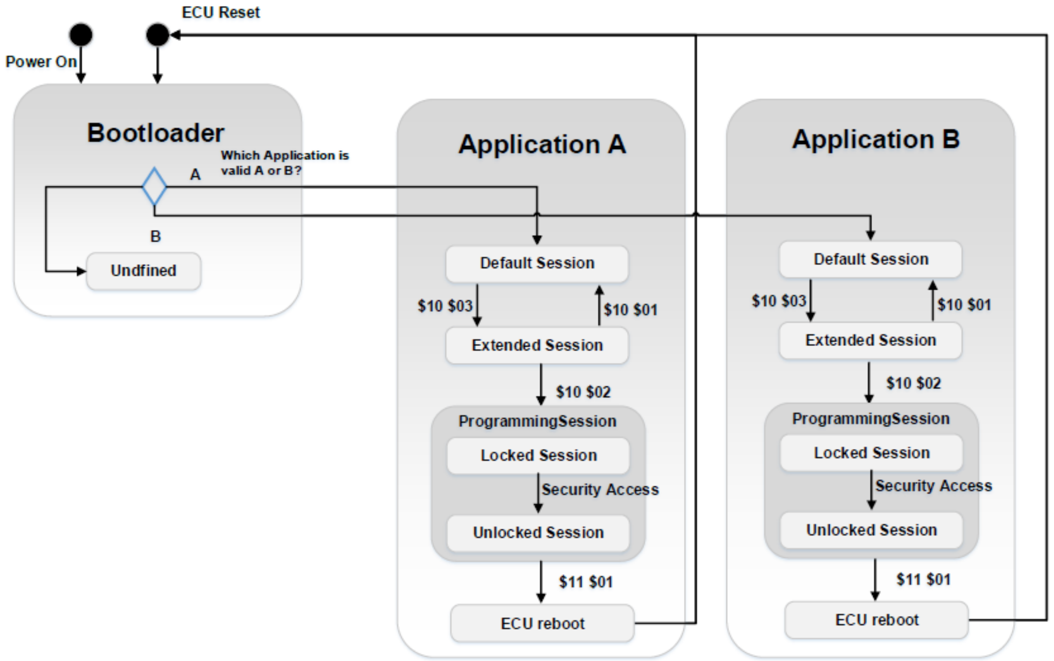
知从科技可以为客户提供 FOTA 完整方案，并可针对项目特定需求和硬件模块定制开发：

ZC can provide customers with a complete FOTA (Firmware Over-The-Air) solution and can customize development according to specific project requirements and hardware modules:

- A/B 区备份升级 A/B partition backup upgrade
- 差分升级 Differential Upgrade
- 备份回滚 Backup rollback
- 无感升级 Seamless upgrade
- 配套上位机工具(玄武上位机工具)
  Supporting upper computer tools (Xuanwu upper computer tool)
- 支持不同 OEM 厂家规范
  Support for different OEM manufacturer specifications

随着越来越复杂的软件功能，在软件升级更新过程中，保证软件能够通过无线升级以及软件回滚功能变得越来越重要。

As software functionality becomes increasingly complex, ensuring that software can be updated through wireless upgrades and that software rollback features are available is becoming more and more important during the software update process.



➢ A/B 区备份升级

A/B Partition Backup Upgrade

传统升级过程中，旧的应用程序通常会被新的应用程序覆盖，当升级过程失败或中断时由于旧的应用程序已经被擦除，此时硬件并不能正常执行应用程序功能，为了避免在升级失败后应用程序失效，通过应用 A/B 分区备份升级功能，旧的应用程序在升级过程中可以进行回滚，保证了应用软件的可靠性；另一方面，A/B 分区备份升级功能可以使应用软件在运行过程中进行升级，改善了用户的使用体验，极大提高了应用软件的升级效率。

In traditional upgrade processes, the old application is usually overwritten by the new one. If the upgrade process fails or is interrupted, and the old application has already been erased, the hardware cannot execute the application function normally. To avoid the application becoming ineffective after an upgrade failure, the A/B partition backup upgrade feature allows the old application to be rolled back during the upgrade process, ensuring the reliability of the application software. On the other hand, the A/B partition backup upgrade feature allows the application software to be upgraded while it is running, improving the user experience and greatly increasing the efficiency of the application software upgrade.

- 差分升级
  Differential Upgrade

差分升级又称增量升级，是通过差分算法将源版本与目标版本之间差异的部分提取出来制作成差分包，然后在设备通过还原算法将差异部分在源版本上进行还原从而升级成目标版本的过程。 差分升级方案不仅可以节省 MCU 内部的资源空间、还可以节省下载流程及下载和升级过程中的功耗。

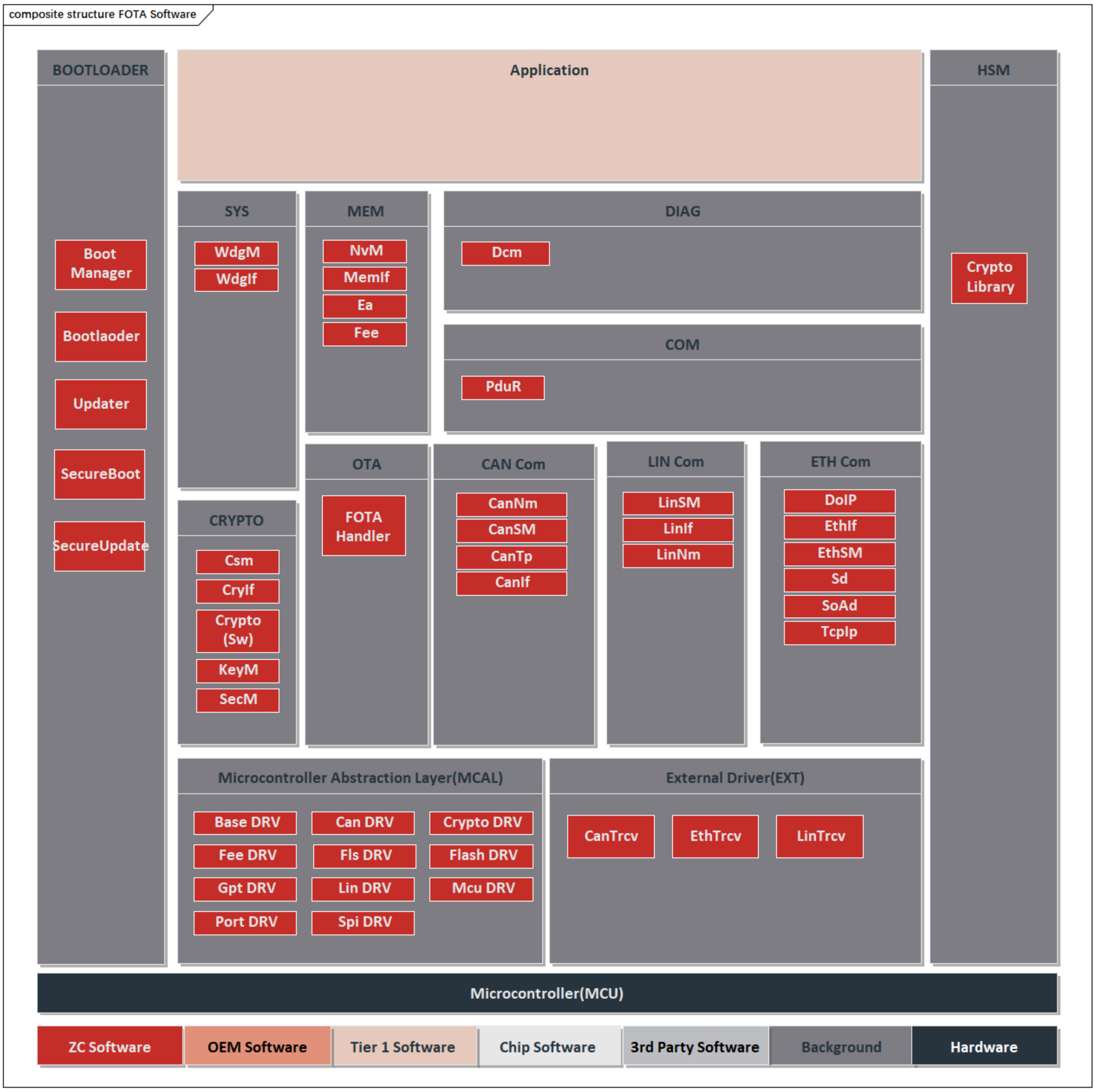
Also known as incremental upgrade, differential upgrade is the process of extracting the differences between the source version and the target version using a differential algorithm to create a differential package. The device then uses a restoration algorithm to restore the differences on the source version, thus upgrading to the target version. The differential upgrade solution not only saves MCU internal resources and space but also saves on the download process and the power consumption during downloading and upgrading.

- 无感升级
  Seamless Upgrade

知从青龙 FOTA 通过与应用程序结合，实现无感升级功能。车辆应用软件通过版本对比、获取升级任务、并自动完成下载，在应用软件运行的过程中下载最新软件数据，完成无感下载。应用软件在完成下载后，将最新软件数据安装到 B 系统，这一过程是在车辆运行时执行完成的，即无感安装。最后，车辆重新上电时，设备执行 AB 区切换，这一过程是激活过程，这一过程是能感知到的过程。对具备“无感升级”能力的设备升流程而言，用户能感知到的过程，仅为新软件系统“激活”的过程。耗时可能达数十分钟的 B 系统切换，在“无感升级”的情况下，

可以大大缩短集成了复杂功能的域控设备的车辆用户可感知的升级时间，减小了驻车升级时对车辆电量的消耗、缩短了客户的车辆不可用时间，也保证了系统本身始终的可用性。

ZC.Qinglong FOTA, by integrating with the application, achieves a seamless upgrade function. The vehicle application software automatically completes the download of the latest software data through version comparison and obtaining upgrade tasks, while the application is running, completing a seamless download. After the application software completes the download, it installs the latest software data into the B system, which is executed while the vehicle is running, i.e., seamless installation. Finally, when the vehicle is powered on again, the device performs an A/B partition switch, which is the activation process, a perceptible process. For devices with "seamless upgrade" capabilities, the process that users can perceive is only the "activation" of the new software system. The B system switch, which may take tens of minutes, can be greatly shortened in the "seamless upgrade" scenario, reducing the power consumption of the vehicle during the upgrade, shortening the customer's vehicle downtime, and ensuring the system's constant availability.



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.

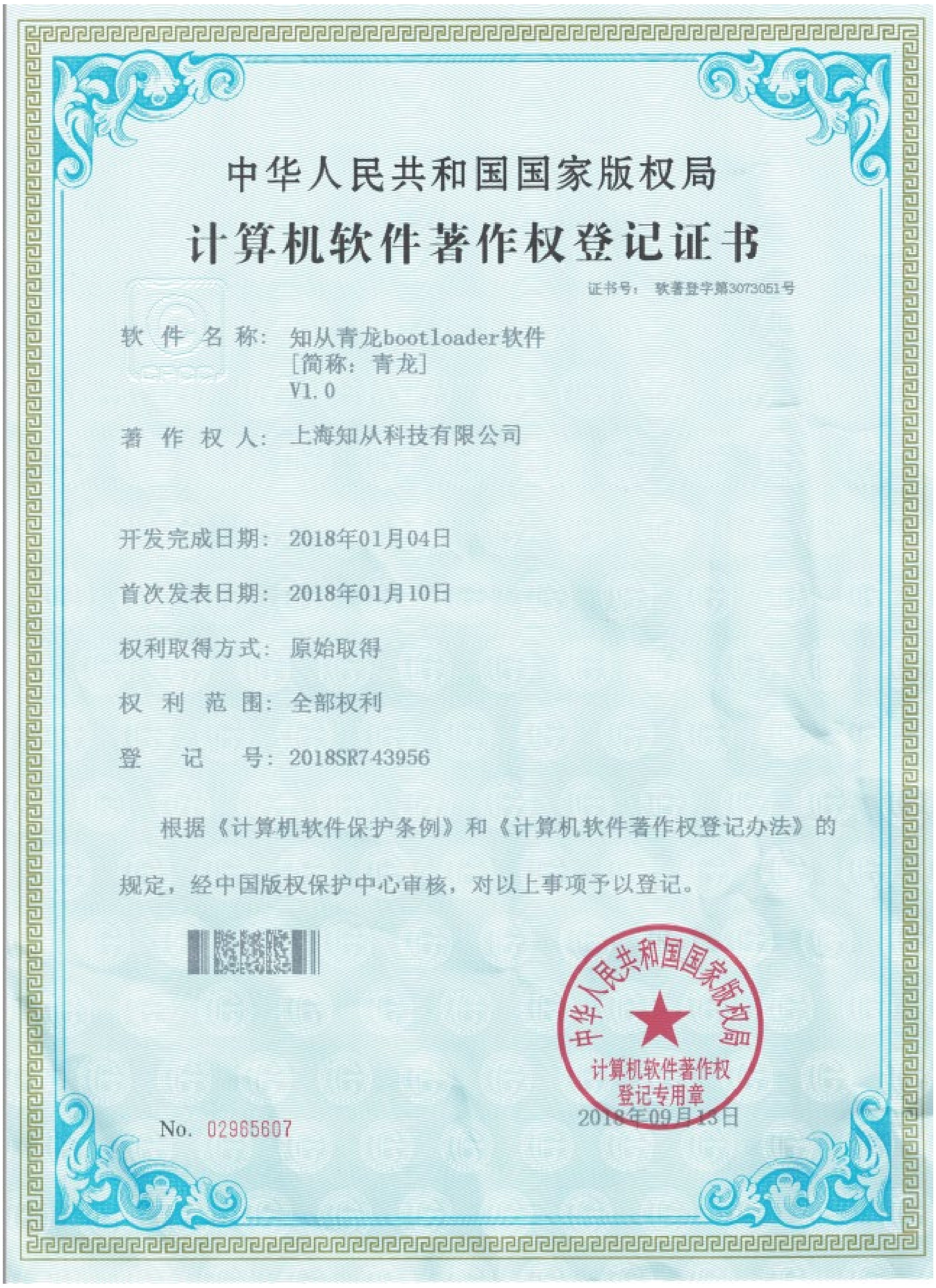
- Dcm

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 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 BOOTLOADER 产品证书
QINGLONG SOFTWARE BOOTLOADER PRODUCT CERTIFICATE