1040605 OTA安全方案

1 概述

1.1 背景

随着安全问题的日益突出，各国政府纷纷出台了一系列法律法规来规范网络行为、保护个人隐私和数据安全。这些法律法规的完善为安全需求的提出和实施提供了法律依据和保障。同时，法律法规的严格执行也促使企业和个人更加重视安全问题。

随着人们生活水平的提高和安全意识的增强，社会对安全问题的关注度不断提高。无论是个人用户还是企业组织，都期望能够在一个安全、可靠的环境中使用技术和服务。这种期望促使技术提供者和服务提供商不断提升自身的安全能力和水平。

企业内部资产是企业投入了大量的人力财力创造出来的成果，需要得到保护，防止被盗取并用于非法用途，需增加相应的机制防止资产流程或被破解。

综合上OTA也需要再该业务领域增加安全设计，保证资产安全。

1.2 目的

此文档的主要目的为明确“汽车OTA管理平台”与汽车端所必须具备的信息安全方案，详细描述各安全方案的设计、功能定义、功能逻辑等。以供相关人员参阅。

PS：不同车厂，对于PKI体系的搭建方式、实现的程度，不同，因此我们整体的安全方案，均需要在车厂当前PKI体系的实际情况，进行灵活的调整，并提出我们对于安全方案的理解。

1.3 简介

本文档主要介绍了，汽车OTA所涉及的信息安全方案，其中主要包含：升级包安全方案、车云链路安全、车内链路安全、车辆安全存储等方案，分别从车、云为实现信息安全，所采用的具体方案描述。

1.4 范围

此文档应用于“汽车OTA管理平台”、UC-Master公版项目开发工作。本文档主要读者为开发人员、测试人员、设计人员（UE、UI）等。

1.5 引用

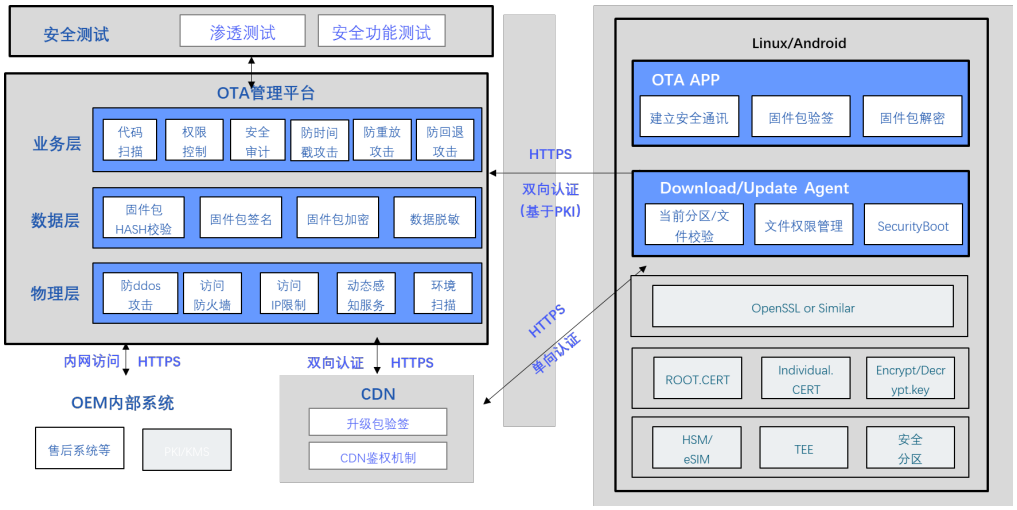
从信息安全层面，OTA安全防护主要包含：云端安全，车端安全，通信链路安全，业务安全等几个方面；

云端安全：安全的操作流程，流程的安全审计，安全的运行环境；

车端安全：安全的存储，安全的Boot，安全的运行环境；

链路安全：APN私有网络，X.509证书，TSL1.2及以上安全协议；

业务安全：完善的权限管理及认证体系，升级包及数据的安全保护，安全合规测试；



本地文档主要介绍升级包安全方案和通讯安全。

1.6 术语

缩写/术语	释义
非对称加密	非对称加密算法需要两个密钥：公开密钥（publickey:简称公钥）和私有密钥（privatekey:简称私钥）。公钥与私钥是一对，如果用公钥对数据进行加密，只有用对应的私钥才能解密，如果使用私钥对数据加密，只有使用公钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫作非对称加密算法。
私钥	私钥指在非对称加密中，由用户自己保存的密钥，该密钥不可被泄露。
公钥	公钥指在非对称加密中，公开发布的密钥。
CA证书	CA是证书的签发机构，它是公钥基础设施（Public Key Infrastructure，PKI）的核心。CA是负责签发证书、认证证书、管理已颁发证书的机关。 CA 拥有一个证书（内含公钥和私钥）。网上的公众用户通过验证 CA 的签字从而信任 CA ，任何人都可以得到 CA 的证书（含公钥），用以验证它所签发的证书。 如果用户想得到一份属于自己的证书，他应先向 CA 提出申请。在 CA 判明申请者的身份后，便为他分配一个公钥，并且 CA 将该公钥与申请者的身份信息绑在一起，并为之签字后，便形成证书发给申请者。 如果一个用户想鉴别另一个证书的真伪，他就用 CA 的公钥对那个证书上的签字进行验证，一旦验证通过，该证书就被认为是有效的。证书实际是由证书签证机关（CA）签发的对用户的公钥的认证。
对称加密	采用单钥密码系统的加密方法，同一个密钥可以同时用作信息的加密和解密，这种加密方法称为对称加密，也称为单密钥加密。 常用的加密算法有：AES、DES、3DES、TDEA、Blowfish、RC2、RC4、RC5、IDEA、SKIPJACK
AES	高级加密标准，是下一代的加密算法标准，速度快，安全级别高，支持128、192、256位密钥的加密；
TLS	安全传输层协议（TLS）用于在两个通信应用程序之间提供保密性和数据完整性

1.7 方案列表

1.7.1 升级包安全

- 升级包身份认证，基于PKI 的升级包签名方案，依赖第三方CA机构提供证书
- 升级包防泄漏，基于PKI的升级包加密方案，对称加密加密算法为AES 256
- 升级包防泄漏，基于PKI的密钥数字信封方案，依赖第三方CA机构提供证书

1.7.2 车云链路安全

- 车云链路安全，HTTPS 双向认证方案，依赖第三方CA机构提供证书
- CDN链路安全，HTTPS 单向认证方案，依赖第三方CA机构提供证书

1.7.2 车内链路安全

- USB/以太网通道（APRC），ARPC协议安全，车辆OTA组件部署在不同域控下的通信安全方案，依赖第三方CA机构提供证书

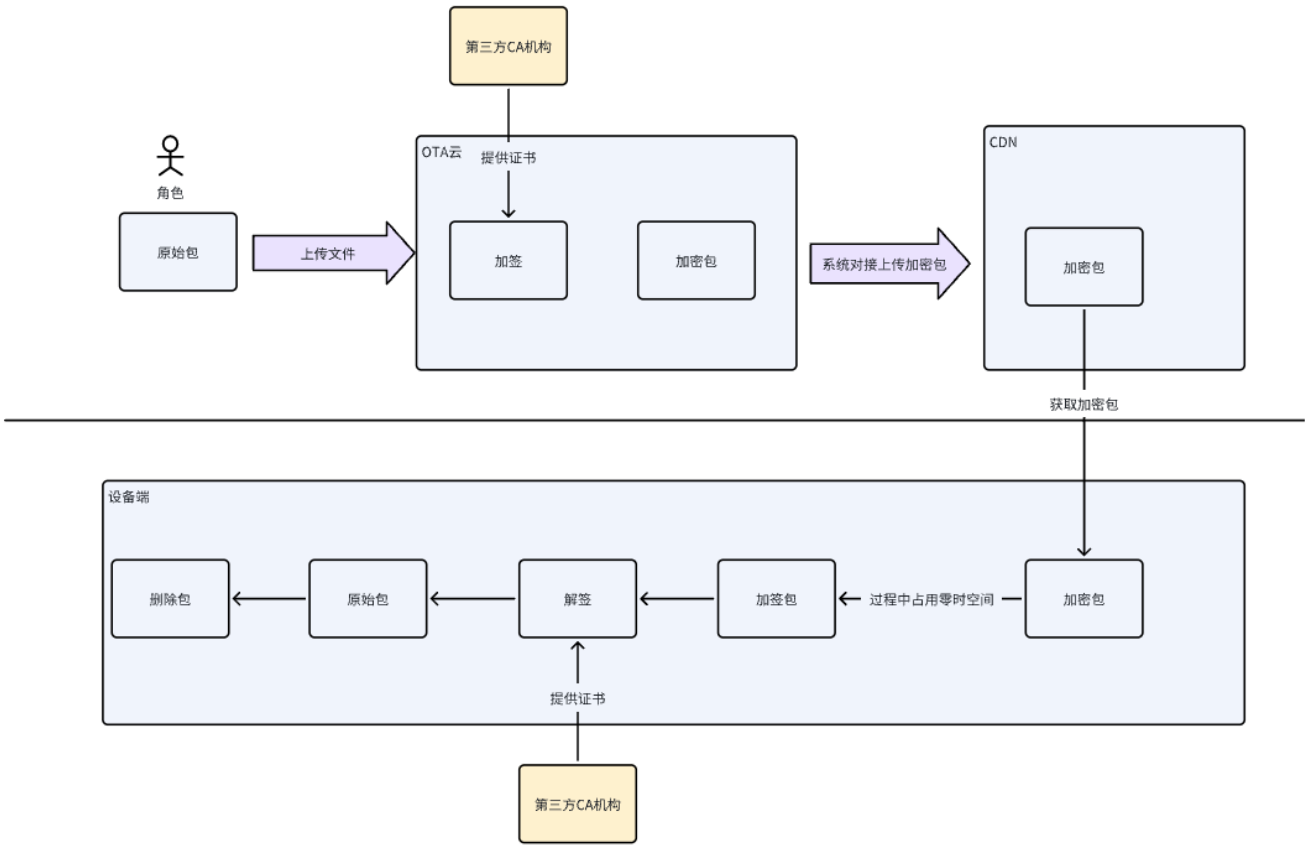
2 规格说明

2.1 升级包安全

升级包安全方案，主要从两个角度，对升级包的安全进行保证：

1. 升级包合法性认证：主要是为了保证，升级包是由车厂或供应商提供的合法的升级包，防止升级包被人为篡改为不明来路的升级包，车辆升级失败所导致的安全隐患，所以在车辆下载完升级包，触发升级前，对升级包合法性进行校验。当前我们采用的主要认证方式：对升级包进行数据签名的方式实现，这种数字签名并验证的能力，一般由第三方安全厂商实现，也可由艾拉比实现，但需要主机厂提供相关的技术支持。
2. 升级包加密：主要是为了保证，升级包地址被破解获取，被非法下载导致的文件泄露，加密后的升级包，无法被正常使用。当前升级包加密的方案，是采用对称加密的方式，对升级包进行加密，车端下载完成升级包，对升级包解密后使用，这种升级包加密的能力，一般由第三方安全厂商实现，也可由艾拉比实现，但需要主机厂提供相关的技术支持。

升级包在业务中的流转过程如下：



2.1.1 升级包签名方案

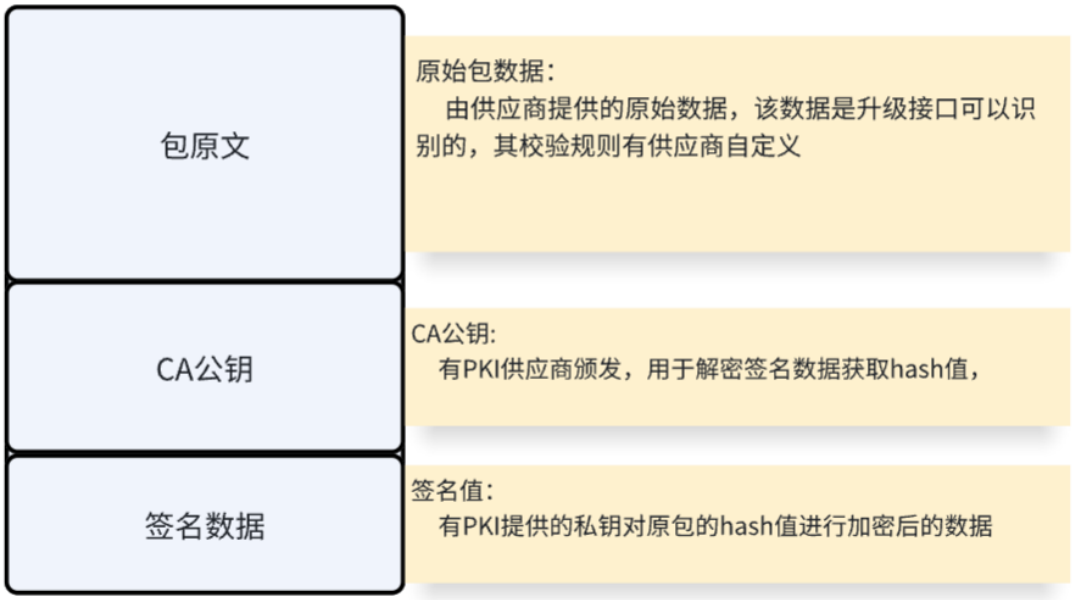
- 签名方案基本原理
    - 公钥与私钥说明：

由于私钥是，是交由使用者保管，而公钥是公开的，可以被任何人使用，被私钥加密过的文件，只有公钥能解开，因此，当成功，即可认为数据是A方发过来的，合法数据。

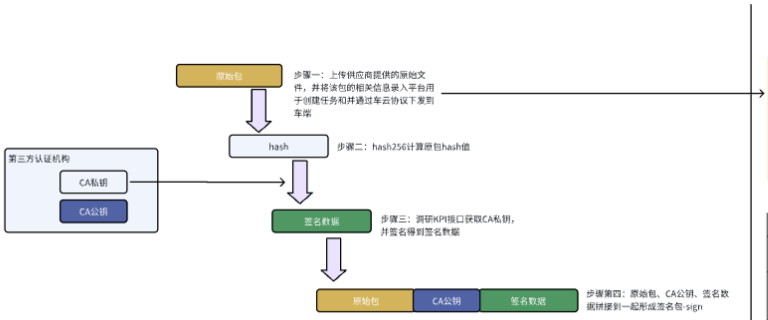
- 方案前提：

1. 主机厂需向第三方CA机构，申请验签所需的公钥证书、私钥证书、CA公钥证书；
2. 云端集成，用于签名的私钥；
3. 车端集成，用于验证签名公钥证书合法性的CA公钥证书；
4. 验签公钥证书，跟随升级包下发至车端；
    - 流程说明：
5. 签名：
    a. 升级包在发布后，需要计算升级包的HASH值，并通过验签私钥对升级包的hash值进行非对称加密算法加密，生成签名信息；
    b. 云平台将：签名、公钥、升级包进行打包处理，将签名、公钥、升级包进行文件拼接，将签名、公钥拼接在升级包的头信息中，生成升级包-sign文件，并将其下发到车端。
6. 验签：
    a. 车端接收到升级包-sign文件后，根据云端下发的升级包、签名大小，对文件进行拆解成升级包、签名、公钥（证书）。
    b. 使用CA公钥证书，对公钥（证书）进行验签。
    c. 使用公钥对升级包的签名进行解密出hash1，同时对升级包计算hash2，比对hash1和hash2，如果hash1和hash2一致，则认定为升级包是合法的，验签结束。
7. 签名分工：
    a. 云端：
        i. 负责升级包签名的触发；
        ii. 负责升级包与签名、公钥组装为：升级包-sign；
    b. 车端：
        i. 负责将升级包-sign，拆解为：升级包、签名、公钥；
        ii. 负责触发升级包验签
    c. PKI：
        i. 云端：
            1. 提供PKI SDK，供OTA管理平台调用，对升级包做签名；
            2. 返还OTA管理平台，公钥、签名信息；
            3. 管理签名所需的算法、证书等；
        ii. 车端：
            1. 负责提供PKI SDK，供OTA SDK 调用，验签升级包；
            2. 返回验签结果，给到OTA SDK；
            3. 管理验签所需的算法、证书等（证书1）；

升级包-sign文件格式：

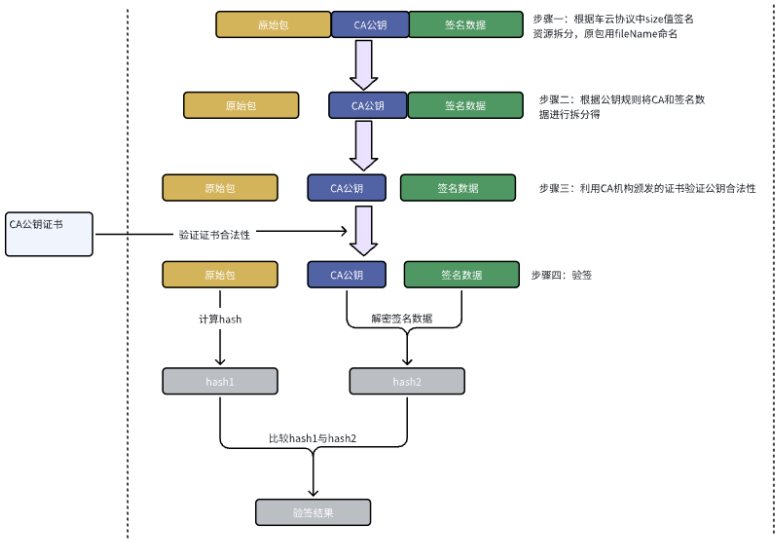


1、签名包制作流程



fileName	String	是	文件名称
url	String	是	文件下载 Url
hash	String(150)	是	文件 Hash 算法：SHA256
size	Long	是	文件大小 单位：Byte
fileSecurityInfo	Object	否	文件安全保护相关

2、签名包验签流程



车云协议

fileName	String	是	文件名称
url	String	是	文件下载 Url
hash	String(150)	是	文件 Hash 算法：SHA256
size	Long	是	文件大小 单位：Byte
fileSecurityInfo	Object	否	文件安全保护相关

当前OTA市场的升级包验签方案，基本由第三方在车厂内部搭建的PKI安全体系，来提供签名、验签的能力，因此本方案为基于：PKI体系下的安全方案。

2.1.2 升级包加密方案

1. 升级包对称加密方案基本原理：

- 为什么采用对称加密：

采用对称加密，主要是其算法：对于大文件，加密快、解密快，安全系数高等优点，既保证了升级包的安全性，同时保证了升级包加密、解密的时效性；

同时对于密钥的安全，不同厂家也提供了安全的保密方案，包含数字信封、或PKI提供即用即消的密钥查询接口等；、

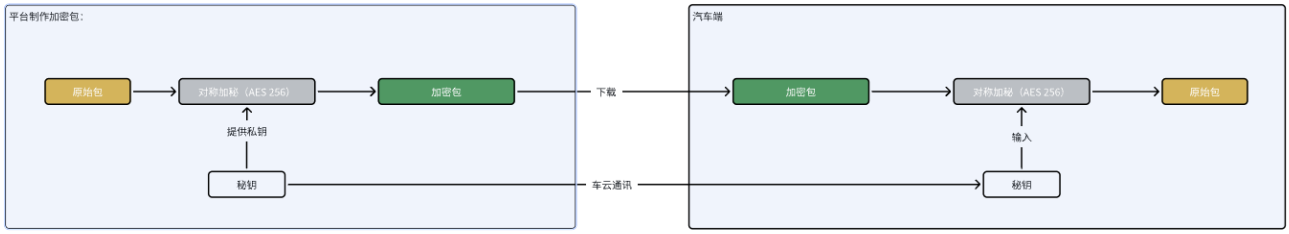
a. 云端：
   i. 负责调用PKI SDK，获取密钥；
   ii. 负责使用密钥，采用AES 256对升级包加密，获取加密包；
   iii. 存储加密包，并存储升级包密钥，并将加密包、密钥下发给车；
b. 车端：
   i. 负责调用PKI SDK，获取密钥；
   ii. 负责使用密钥，采用AES 256对加密包解密，获取升级包；

- PKI安全厂商：

a. 云端：
   i. 负责提供PKI SDK，供OTA管理平台调用，获取密钥；
   ii. 负责对密钥进行管理；
b. 车端：
   i. 负责提供PKI SDK，供OTA SDK 调用，获取密钥；

- 流程说明：

1. 加密流程：
   a. 云平台生成密钥（唯一），将升级包通过对称加密算法，加密为加密包；
   b. 云平台将加密包、密钥，下发给到车端；
2. 解密流程：
   a. 车端使用从平台获得的密钥，对加密包，通过对称加密算法，解密为升级包；

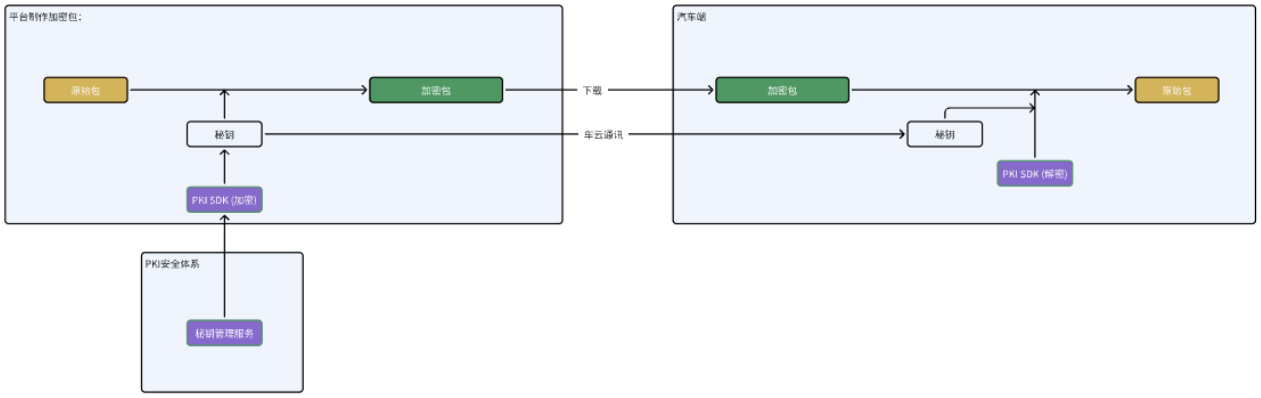


2、为基于PKI体系下的安全方案：

a. 云端：
   i. 负责调用PKI SDK，获取密钥；
   ii. 负责使用密钥，采用AES 512对升级包加密，获取加密包；
   iii. 存储加密包，并存储升级包密钥，并将加密包、密钥下发给车；
b. 车端：
   i. 负责调用PKI SDK，获取密钥；
   ii. 负责使用密钥，采用AES 512对加密包解密，获取升级包；

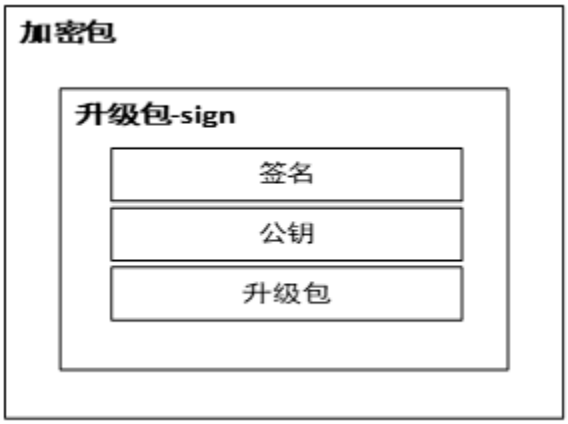
- PKI安全厂商：

a. 云端：
   i. 负责提供PKI SDK，供OTA管理平台调用，获取密钥；
   ii. 负责对密钥进行管理；
b. 车端：
   i. 负责提供PKI SDK，供OTA SDK 调用，获取密钥；



2.1.3 结合升级包签名、加密的整体方案

升级包安全是一个整体方案，因此需要对升级包签名\验签、加密\解密进行功能整合，如下图是一个升级包经过签名加密后的结构图：



升级包经过签名加密后的结构图

如图所示：

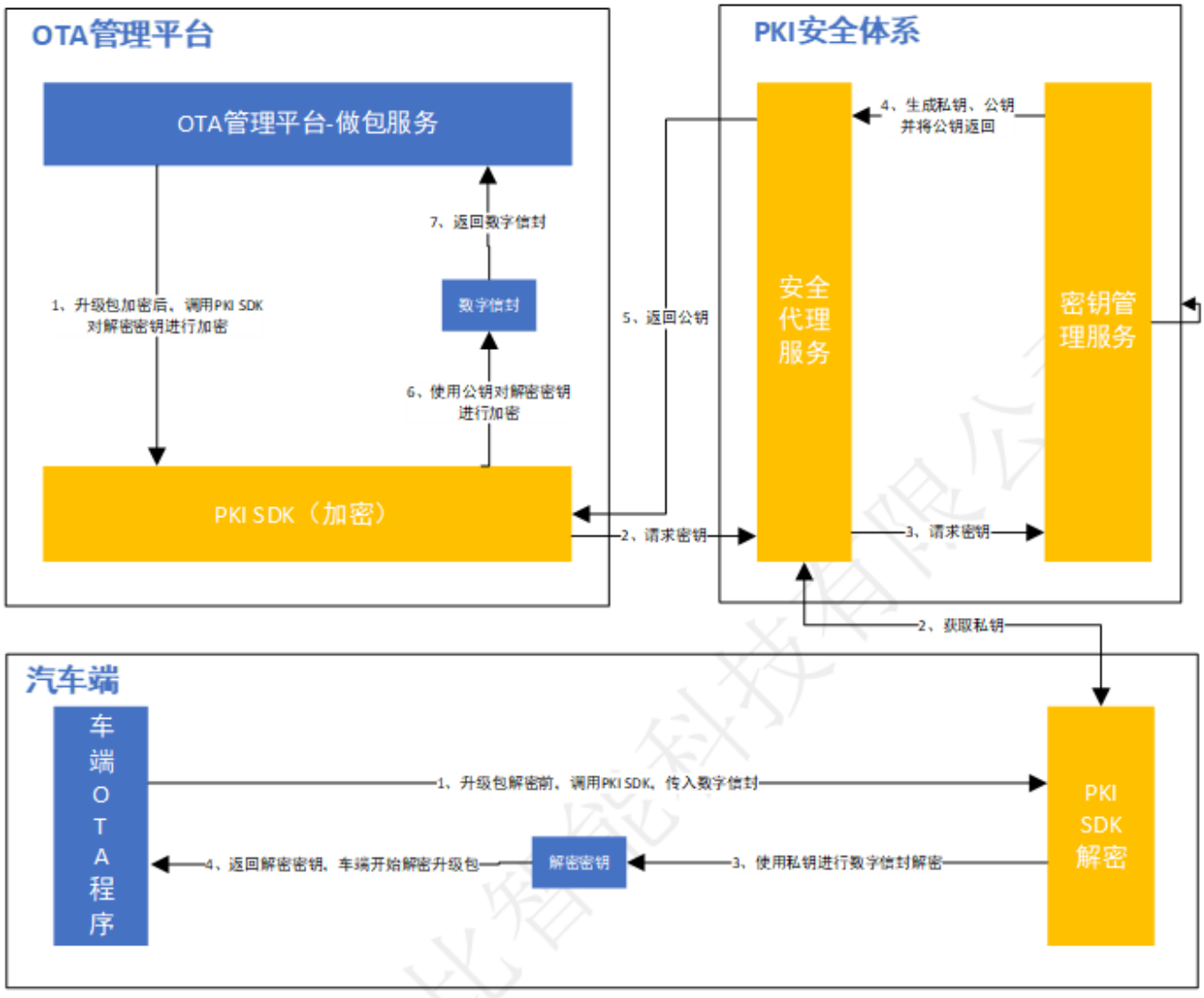
1. 云端下发的是一个加密包；
2. 解密之后，是携带签名、公钥、升级包的：升级包-sign；
3. 经过系统拆解后，可拆解为：签名、公钥、升级包；

因此，升级包先经过签名，再进行加密的操作，在车端处理升级包时：

1. 由于升级包加密，是为了防止下载地址被泄露获取，导致的安全风险，因此，升级包下载完成后，对加密包，进行解密操作。
2. 签名是对一个升级包的合法性的认证，因此，在安装之前，会将升级包sign拆解为：签名、公钥、升级包，并对升级包验签，来保证升级包合法、未被篡改。

1.1.1 加密包密钥数字信封方案（可选）

数字信封，主要指对加密包的密钥，再次采用非对称加密的方式，进行加密，获得数字信封，最终下发到车端，以保证升级包密钥的安全性，整体流程如下图：



- 基于PKI体系下加密包解密密钥数字信封方案

1. 流程说明：
    - 数字信封生成：
        - 升级包加密之后，调用PKI SDK 对解密密钥进行加密；
        - PKI SDK请求安全代理服务，获取加密公钥；
        - 安全代理服务通知密钥管理服务，获取加密公钥；
        - 密钥管理系统，生成公钥、私钥，并将公钥返回给安全代理服务；

        - 安全代理服务，将公钥返回给PKI SDK；
        - PKI SDK使用公钥，通过非对称加密算法，对升级包解密密钥进行加密，为数字信封；
        - 将数字信封，返还给OTA管理平台，OTA管理平台进行存储；
    - 数字信封解密：
        - 在升级包解密之前，车端OTA程序接收由云端下发的数字信封，并调用PKI SDK进行数字信封解密。
        - PKI SDK通过安全代理服务，到密钥管理服务，获取对应的私钥。
        - PKI SDK 通过获得的私钥，对数字信封解密，获取解密密钥。
        - PKI SDK 将解密密钥，返还给车端OTA程序，车端OTA程序，开启对应某一个升级包的解密动作；
        - 数字信封使用的条件：
            - 车厂需要具备完善的PKI管理体系，来管理用于制作数字信封的密钥对；
            - 数字信封，主要是为了防止，对称加密的密钥，泄露，考虑到即用即销的原则，也可以由PKI暴露服务接口，查询指定的密钥，即所有的密钥全部在密钥管理系统中，需要即获取，也能达到同样的效果，因此未必需要数字信封的加密，该方案为可选项；

2. 分工：
    a. 云端：
        i. 负责调用PKI SDK，对对称密钥做加密；
        ii. 存储数字信封，并下发给车；
    b. 车端：
        i. 负责调用PKI SDK，传入数字信封，对数字信封做解密；

    - PKI安全厂商：

        i. 云端：
            1. 负责提供PKI SDK，供OTA管理平台调用，制作数字信封；
            2. 数字信封制作完成后，返回加密结果、数字信封给到OTA管理平台；
            3. 负责对非对称密钥、对加密算法进行管理；
        ii. 车端：
            1. 负责提供PKI SDK，供OTA SDK 调用，解密数字信封；
            2. 将解密包的解密结果、对称密钥，返回给OTA SDK；
            3. 负责对解密算法进行管理；

2.2 车云链路安全方案

车云链路方案主要指，OTA升级过程中，会与部分云端，如：OTA管理平台、CDN进行数据交互，就如何保证该交互过程中的数据安全，所定义的这部分的安全方案。

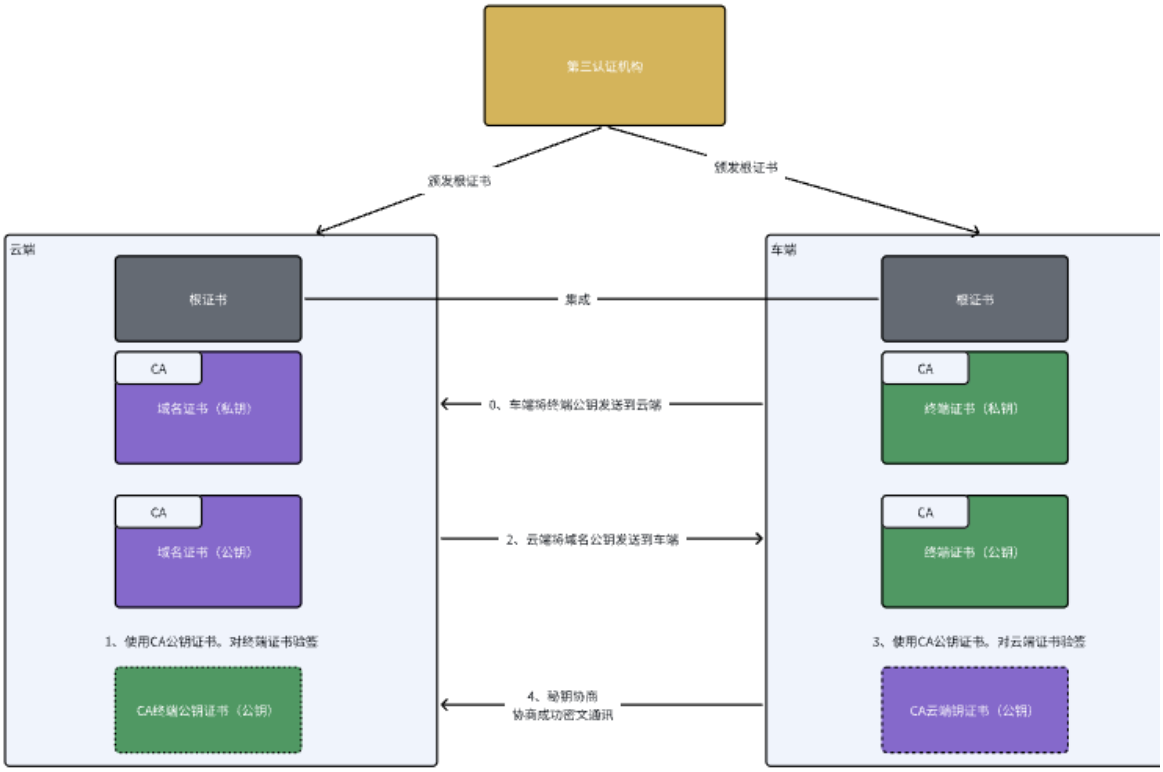
安全方案主要从两个安全进行描述：数据加密（防止传输过程中的泄露）、身份认证（认证交互双方的身份）。

同时，由于在车云交互时，网络存在分层结构，如HTTPS传输层使用标准的TLS安全传输层协议（包含：数据加密、身份认证），艾拉比集成方案，将采用TLS1.2版本以上；

2.2.1 车辆与OTA管理平台 TLS双向认证方案

1. 基本流程说明：

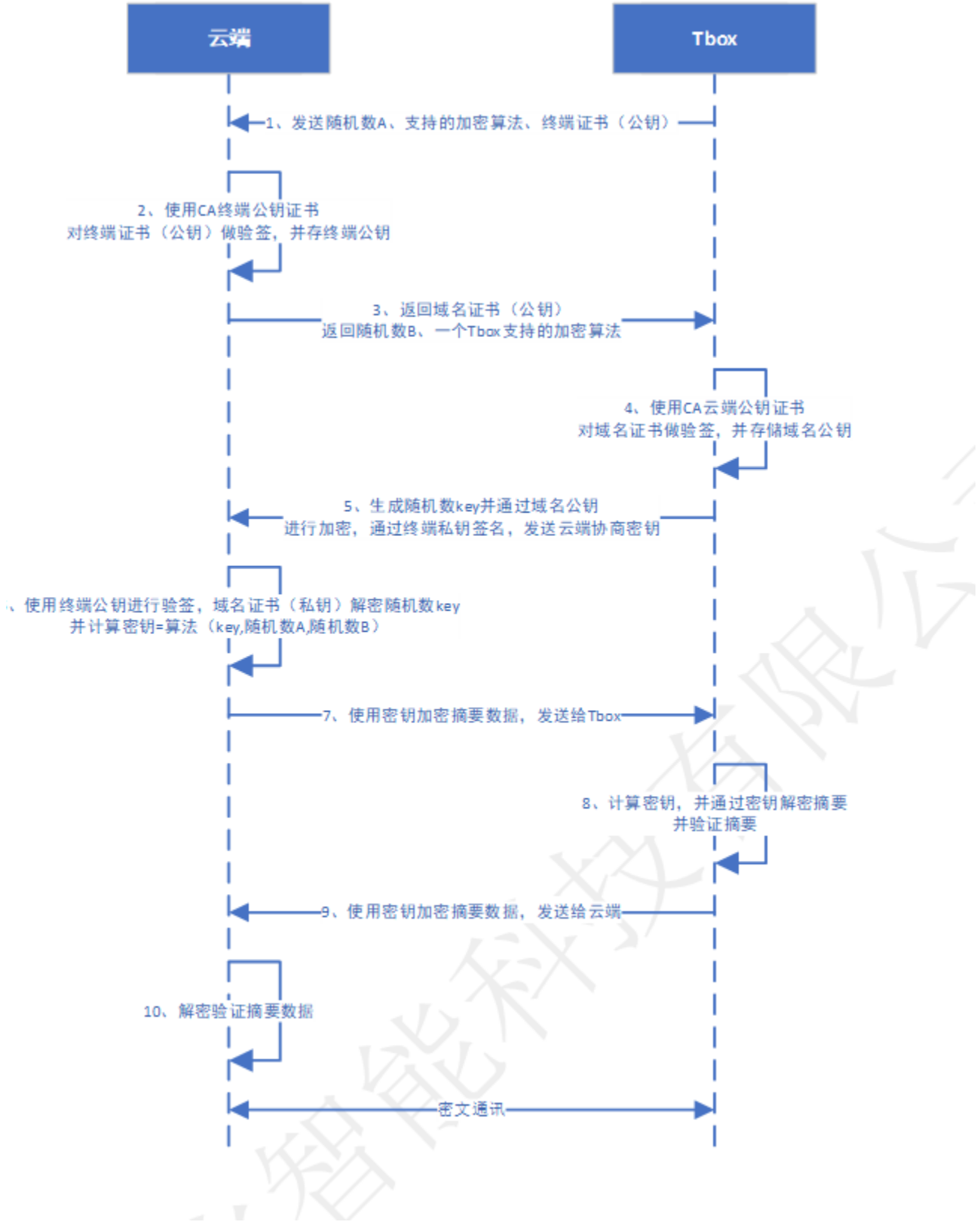
TLS双向认证，主要指车辆在进行一次HTTP请求时，由车端来认证服务器的身份，同时服务端也来认证车端的身份，是否是合法的，整体的方案及流程如下图：



如图所示：

- 准备工作：

1. 主机厂应向第三方申请，域名证书，集成在服务端，用于TLS云端认证；
2. 主机厂应向第三方申请，终端证书，集成在车端，用于TLS车辆认证；
3. 车端需要集成CA提供的云端公钥证书；
4. 云端需要集成CA提供的终端公钥证书；
    - 基础流程说明：
5. 车端发起一次https的业务请求，将终端证书（公钥）发送给云端；
6. 云端通过CA终端公钥证书，对终端证书（公钥）进行验签；
7. 云平台将域名证书（公钥）下发给车端；
8. 车端使用自身集成的CA云端公钥证书，对域名证书，进行身份认证；
9. 如果认证成功，开始协商密钥，进行密文数据通讯；
10. 详细流程说明：



TLS双向认证详细流程图

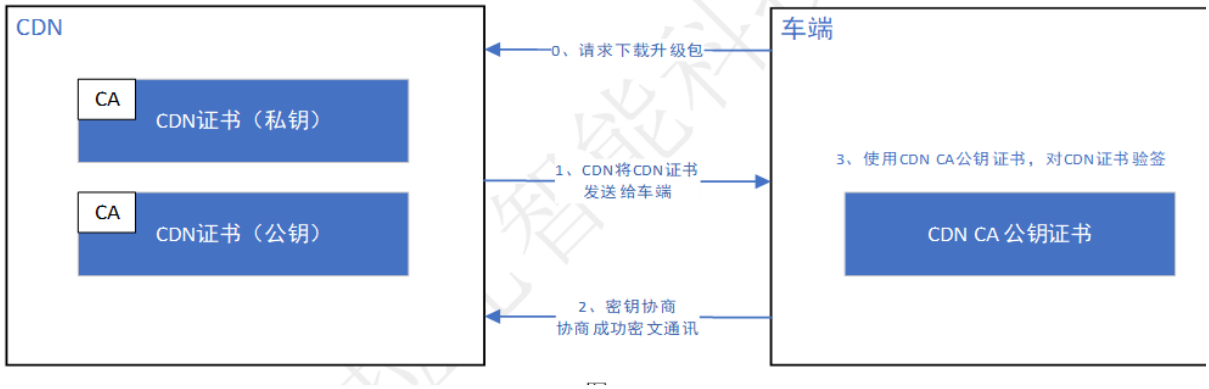
如图所示：

- Tbox终端发送随机数A、支持的加密算法、终端公钥证书给到云端。

- 云端，使用CA终端公钥证书，验签终端公钥证书，成功后存储公钥。
- 云端将使用的域名证书（公钥）、随机数B、一个Tboxe支持的安全算法，下发给到Tbox；
- Tbox使用集成在系统中的CA云端公钥证书，验证域名证书（公钥），合法后将公钥存储到系统中；
- Tbox生成随机数key，并域名证书中的公钥，进行加密，使用终端的私钥证书进行签名，发送给云端协商密钥。
- 云端接收到密钥后，使用终端的公钥对数据进行验签，并使用域名证书（私钥）进行解密，解密后使用key、随机数A、随机数B使用伪随机算法，计算出云端会话密钥和Tbox终端会话密钥；
- 云端，将以上过程中的交互的数据进行摘要运算并使用Tbox终端会话密钥进行加密返回TBox；
- Tbox通过key、随机数A、随机数B使用伪随机算法，计算出云端会话密钥和Tbox终端会话密钥，并使用Tbox终端会话密钥解密获得明文摘要，Tbox对以上过程中的交互的数据进行摘要运算生成摘要值并与解密后摘要值进行校验。校验通过则说明通信双方生成的Tbox终端会话密钥相同；
- Tbox将以上过程中交互的数据进行摘要运算，并使用云端会话密钥进行加密发送给云端；
- 云端，使用云端会话密钥解密获得明文摘要，云端对以上过程中的交互的数据进行摘要运算生成摘要值并与解密后摘要值进行校验。校验通过则说明通信双方生成的云端会话密钥相同。
- 至此TBox终端和云端安全通道正式建立，后续通信双方使用已经协商好的会话密钥对通信双方交互的数据进行加解密，保证通信双方交互数据的网络传输的安全

2.2.2 车辆与CDN 的TLS单向认证方案

车辆在下载升级包时，采用TLS单向认证的方式，即车端认证服务器的合法性方案，原因为，如果要进行双向认证，则CDN必须要集成CA终端公钥证书，但CDN是一个面向多家提供数据分发服务的供应商，相关资源面对其所有服务的客户，如果每家客户均做设备认证，则会带来大量的管理、开发工作，增加维护的复杂性。

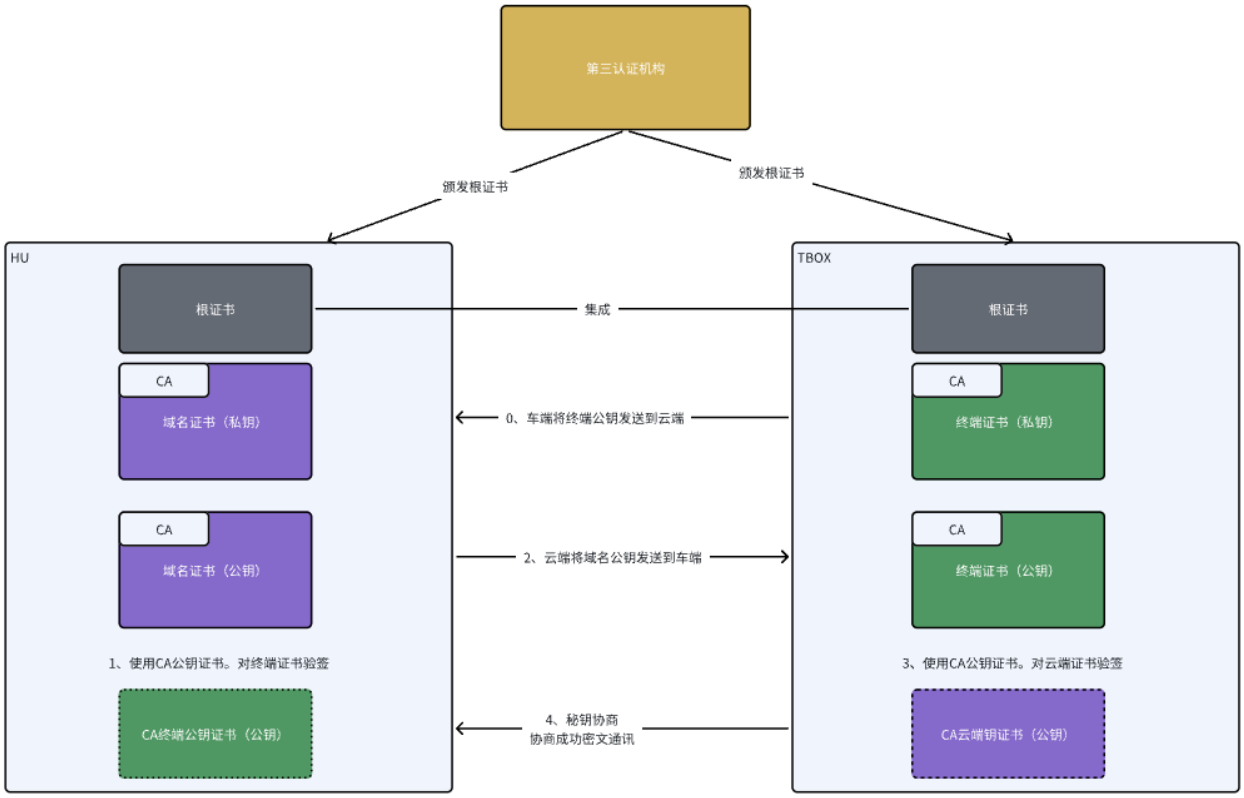


因此，由图所示，CDN采用TLS单向认证，同时需要在车端集成CDN 的CA公钥证书，同时单向认证相比于双向认证，主要是：只做车端认证服务端，服务端不会认证车端的信息，基本流程同3.2.1，只是缺少服务端认证车端的流程。

PS：由于CDN是一个专业提供数据分发平台，其在针对于自身安全上是有专业的安全方案，以上逻辑仅限于参考，具体以项目执行为基准；

2.2.3 USB\以太网通道（ARPC）

ARPC协议，是艾拉比为了实现，在满足车辆OTA功能的场景下，智能件间的数据通讯，所定义的私有协议，该协议可以基于TLS双向认证，来实现零件间通讯的数据加密、身份认证，如下图举例：



- TLS 双向认证

车辆零件间如果需要使用TLS双向认证，需要在零件里分别集成各自所需要的证书：

HU： HU证书（私钥）、HU证书（公钥）、CA 终端公钥证书；

Tbox： 终端证书（私钥）、终端证书（公钥）、CA HU公钥证书；

由于安全证书，在零件间存储，则需要零件供应商，在系统中提供安全存储区域，防止证书泄露，另证书有效期，申请为30年，以贯穿整个车辆生命周期；

在车内零件通讯的过程中，可以互为Server端即，两个零件均可以发起向对方的请求，上图只介绍了Tbox请求HU的场景，HU也可以请求Tbox，基本流程一致