宝能 BAONENG

密级 | 机密

蓝牙钥匙方案

2020-04-20

智能网联研究院

蓝牙钥匙方案

宝能 BAONENG

密级	机密

蓝牙钥匙的定义

1. 基于蓝牙通讯技术的一种数字身份识别和加密通讯技术
2. 蓝牙通讯中用于通讯加密的数字密钥
3. 借助于移动设备实现同被控设备（比如车辆）之间的加密通讯
4. 在用车场景中实现人与车的近场通讯
5. 在用车场景中实现车门解锁/闭锁，车辆启动，车窗开关等控制功能

蓝牙钥匙方案

宝能 BAONENG

密级	机密

蓝牙钥匙存在的价值

1. 物理钥匙数量有限，且存在丢失，损坏的问题
2. 物理钥匙不方便携带
3. 解决物理钥匙不方便多人共享的问题
4. 未来虚拟钥匙将彻底替代物理钥匙，物理钥匙只用于应急
5. 弥补车辆远程控制在无网络信号的环境下无法使用的问题，比如地下车库
6. 弥补远程控车的延时问题，在近场情况下，自动采用近场蓝牙通讯实现控车
7. 车辆租赁和共享的时代离不开虚拟钥匙，离不开近场通讯的虚拟蓝牙钥匙

蓝牙钥匙方案

宝能 BAONENG

密级	机密

技术需求

1. 本方案旨在通过蓝牙通讯技术实现车辆数字钥匙的共享和使用，支持车主用车，家庭用车，朋友借车等多种用车场景
2. 支持车辆停放在无网络信号的环境下的借车和还车
3. 支持蓝牙定位，实现蓝牙测距和车内车外的判断
4. 支持基于蓝牙钥匙的用户身份识别
5. 支持基于蓝牙技术的近场车辆控制
6. 支持针对蓝牙模式的授权与鉴权

蓝牙钥匙方案

宝能 BAONENG

密级	机密

蓝牙钥匙的钥匙规划

1. 一人一车
    1. 一个用户账号在登陆的一台移动设备中，针对某一辆车辆，只允许存在一把钥匙
    2. 一个蓝牙钥匙必须是某个账号针对某台移动设备的蓝牙钥匙
    3. 一个用户账号在不同的设备登录必须申请不同的蓝牙钥匙
    4. 支持一个用户在不同的设备上针对一辆车拥有多把蓝牙钥匙
    5. 移动设备发生变更，丢失等情况时，只能重新申请蓝牙钥匙
2. 一人多车
    1. 一人多车时，不同的车对应不同的蓝牙钥匙
3. 多人一车
    1. 多人共同使用一辆车时，每个人有各自不同的蓝牙钥匙

蓝牙钥匙方案

宝能 BAONENG

密级	机密

蓝牙钥匙使用角色的定义

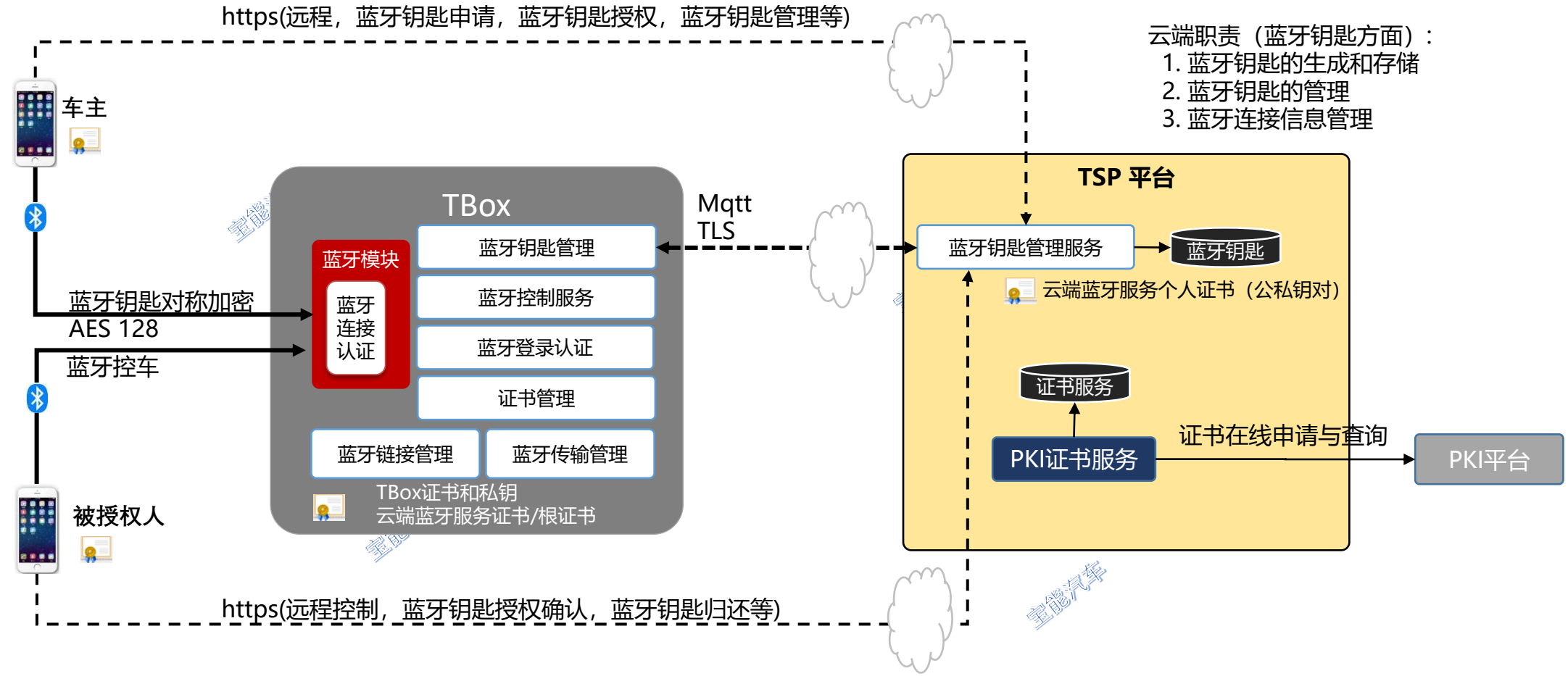
1. 整体上，蓝牙钥匙分为**车主**和**被授权用户**两大角色
    1. 车主拥有对车辆的完全控制权限
    2. 被授权用户可以结合业务需求进一步的细分为多种角色，不同的角色授予不同的权限。
2. 一个用户在不同的车上可能具有不同的角色，在车辆A上是车主，在车辆B上可能是被授权用户

蓝牙钥匙方案

宝能 BAONENG

密级	机密

整体架构



说明： 本架构图仅描述蓝牙钥匙相关的业务架构，蓝牙钥匙依赖的tsp服务，证书申请等，不在本文档详细描述

蓝牙钥匙方案

宝能 BAONENG

密级	机密

技术要点

1. 相关主体
    1. 本方案将以手机App端代表所有具有蓝牙芯片的移动设备App端，简称App
    2. 本方案将以TBox终端代表所有实现蓝牙钥匙功能的终端设备
    3. “蓝牙钥匙”指用于手机App同车辆TBox终端蓝牙通讯过程中的数据加密的对称加密密钥
2. 蓝牙钥匙分为车主和被授权人两大类用户角色
3. 证书
    1. 需要在云端为蓝牙钥匙服务配置蓝牙服务个人证书(公私钥对，可以同其他应用共用证书)
    2. 需要预先在TBox终端安装根证书，TBox个人证书(按PKI规划的流程申请或预置)和云端蓝牙服务公钥证书
    3. 本方案需要在手机App端安装个人证书
    4. 云端需要提供证书公钥查询的接口或能力
4. 蓝牙钥匙
    1. 本方案采用云端生成蓝牙钥匙的方案，云端生成对称钥匙，并分发到TBox和手机App，支持TSP通道和蓝牙通道的两种通道下发的模式
    2. 借助于手机App端证书加强蓝牙钥匙交换环节的安全
    3. 手机App端需要考虑蓝牙钥匙的安全存储 （比如，存在在手机的安全区域）
    4. 充分信任云端，只要是云端的授权签名就认为是一个合法的蓝牙钥匙授权
5. 蓝牙通讯
    1. 支持手机App同TBox的蓝牙通讯的防重放能力
    2. 支持手机App同TBox的蓝牙通讯的超长字节数传输(大于一次蓝牙通讯的最高字节数)

蓝牙钥匙方案

宝能 BAONENG

密级	机密

证书需求

TSP云平台证书：

- 预置平台根证书
- 安装云端蓝牙钥匙服务证书
- 存储TBox, 用户的公钥
- 提供PKI证书服务与管理

TBox证书：

- 预置平台根证书
- TBox需要预置申请证书所需要的证书
- TBox向后台申请TBox证书，或者TBox在出厂前预置证书(证书线下批量生成)
- TBox从云端获得云端蓝牙钥匙服务公钥
- 手机App通过蓝牙将用户公钥传给TBox

用户证书(车主/非车主)：

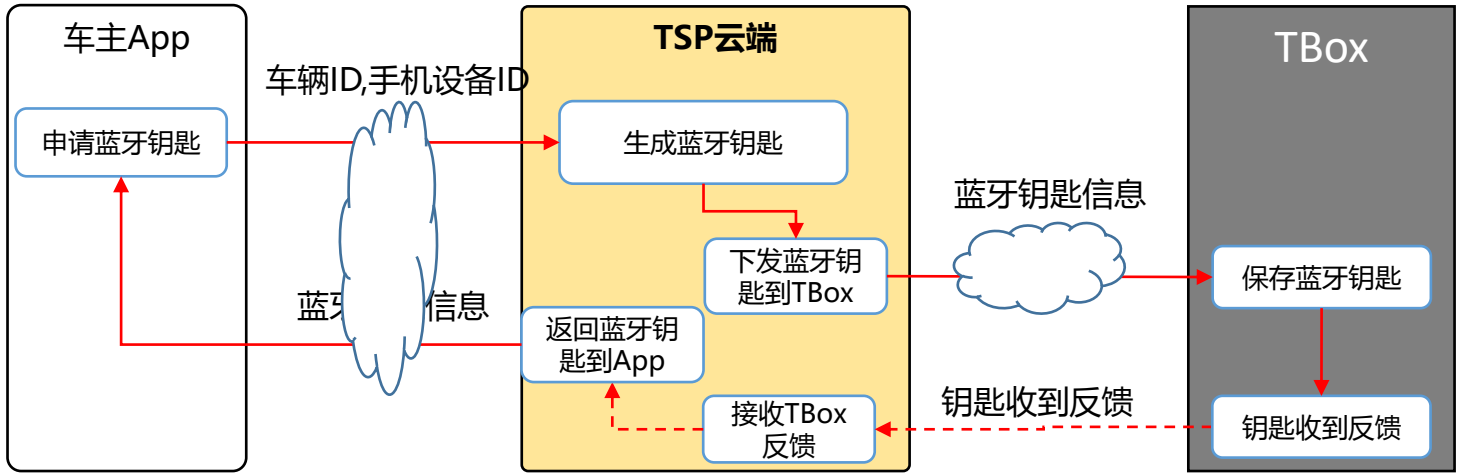
- 预置平台根证书
- 手机App在登录的状态下可以向云端申请个人证书
- 手机App从云端获得云端蓝牙钥匙公钥
- 车主App在开通车辆蓝牙钥匙服务时可以从云端获得车辆的公钥
- 被授权人App在接收到车主借车授权时可以从云端获得车辆的公钥

蓝牙钥匙方案

宝能 BAONENG

密级	机密

车主申请蓝牙钥匙



前提
1. 车主申请蓝牙钥匙首先需要完成车主车辆的绑定
2. 车主申请蓝牙钥匙要求车辆处于有网络信号的环境下

步骤：
1. 车主登录手机App
2. 车主向云端发起蓝牙钥匙开通申请
   参数：车辆ID，手机设备ID
3. 云端生成蓝牙钥匙
   蓝牙钥匙：16字节随机蓝牙钥匙
4. 云端将蓝牙钥及相关信息匙推送到TBox
   1. 采用TBox公钥加密, 加密后生成云端签名
   2. TBox给云端返回蓝牙连接信息
5. 云端将蓝牙钥匙及相关信息返回给手机App
   1. 采用手机App用户公钥加密, 加密后生成云端签名

备注：
1. 蓝牙钥匙在App端和Tbox端以各自公钥加密存储
2. 手机需要确保蓝牙钥匙的安全加密存储
3. TBox端需要确保蓝牙钥匙的加密存储

补充说明：
1. 云端下发给TBox的蓝牙钥匙信息：用户ID，手机设备ID，车主标识，蓝牙钥匙编号，蓝牙钥匙(TBox公钥加密))，蓝牙钥匙生效时间，蓝牙钥匙失效时间，蓝牙钥匙云端签名
2. 云端返回给手机App的蓝牙钥匙信息：车辆ID, 蓝牙钥匙编号，蓝牙钥匙(App公钥加密)，蓝牙钥匙生效时间，蓝牙钥匙失效时间，蓝牙名称，蓝牙pin，蓝牙钥匙云端签名，对
3. 蓝牙钥匙云端签名(云端蓝牙服务证书私钥) : 采用私钥签名算法ECDSA-256 (用户ID+手机设备ID+蓝牙钥匙生效时间+蓝牙钥匙失效时间+蓝牙钥匙（加密态）)

蓝牙钥匙方案

宝能 BAONENG

密级 | 机密

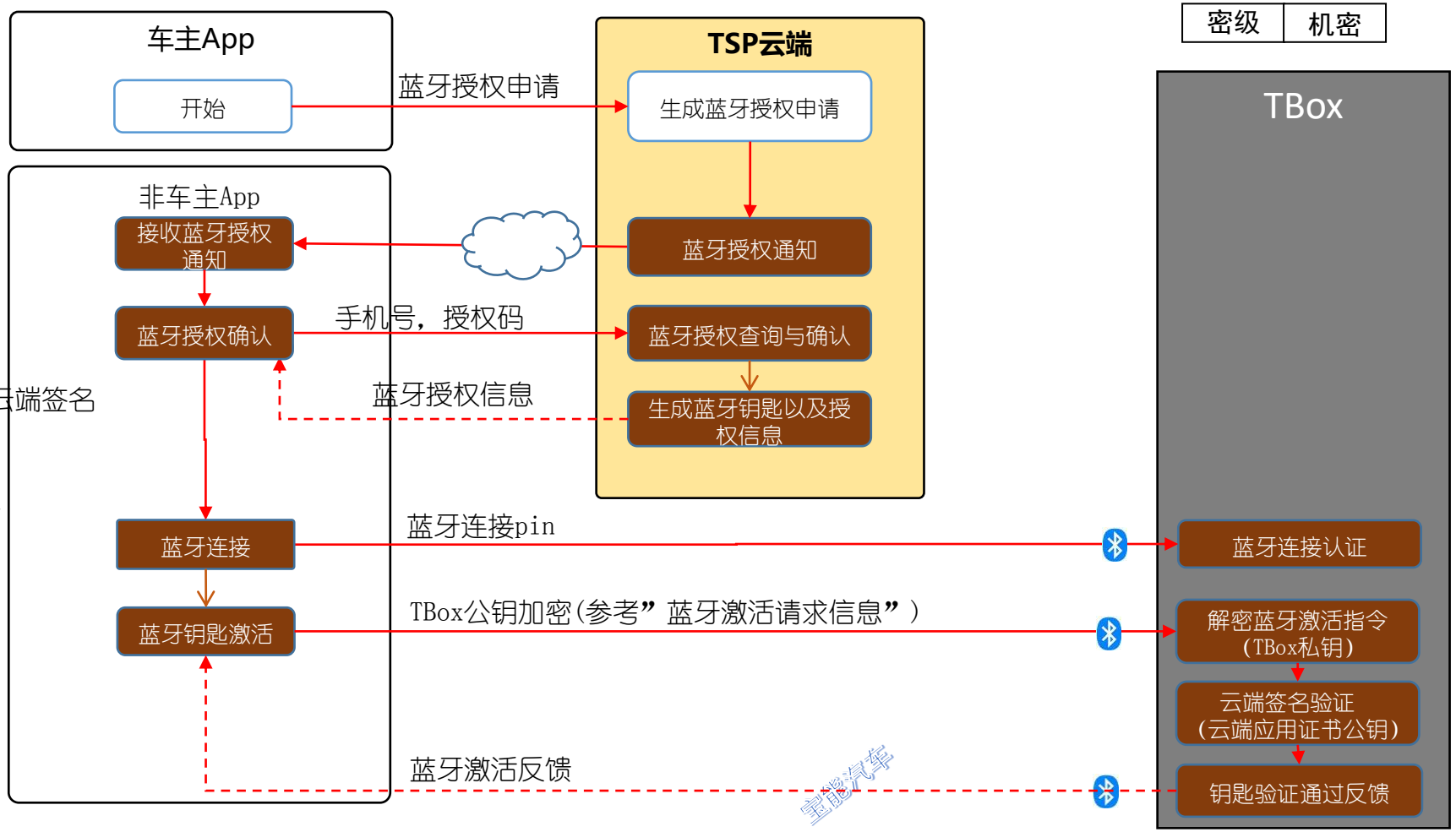
被授权人蓝牙钥匙申请

步骤：

1. 车主发起**蓝牙授权申请**
1. 云端生成**授权码**，创建蓝牙**授权申请记录**
2. 云端向被授权人手机发送蓝牙授权通知
3. 被授权人注册，登录，获取蓝牙授权通知
4. 被授权人进行**蓝牙授权确认**
    1. 云端生成**蓝牙钥匙**
    2. 云端生成**蓝牙授权凭证并签名**
    3. 云端生成**手机App端蓝牙钥匙**
        采用被授权人公钥加密，加密后生成云端签名
    4. 云端生成**蓝牙授权信息**
    5. 将**蓝牙授权信息 以及**返回给被授权人
5. 被授权人App从蓝牙授权信息中获取app蓝牙钥匙
    1. 验证云端签名
    2. 以加密态安全存储蓝牙钥匙
6. 被授权人**激活蓝牙钥匙**
    1. 被授权人连接车辆蓝牙
    2. 被授权借助**蓝牙授权凭证**激活蓝牙钥匙

备注：

1. 蓝牙钥匙在App端和TBox端以公钥加密状态存储
2. 手机需要确保蓝牙钥匙的安全加密存储
3. TBox端需要确保蓝牙钥匙的加密存储
4. 蓝牙钥匙在云端需要加密存储

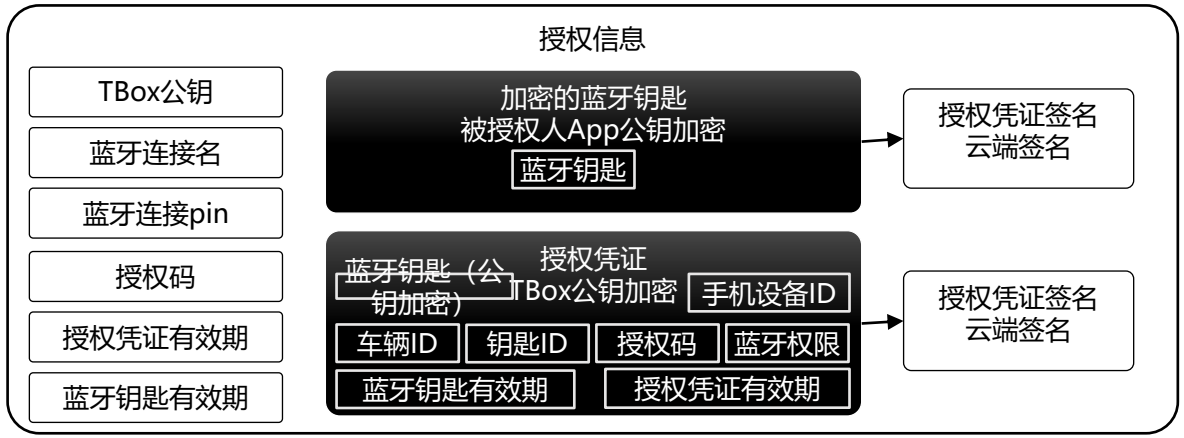


补充说明：

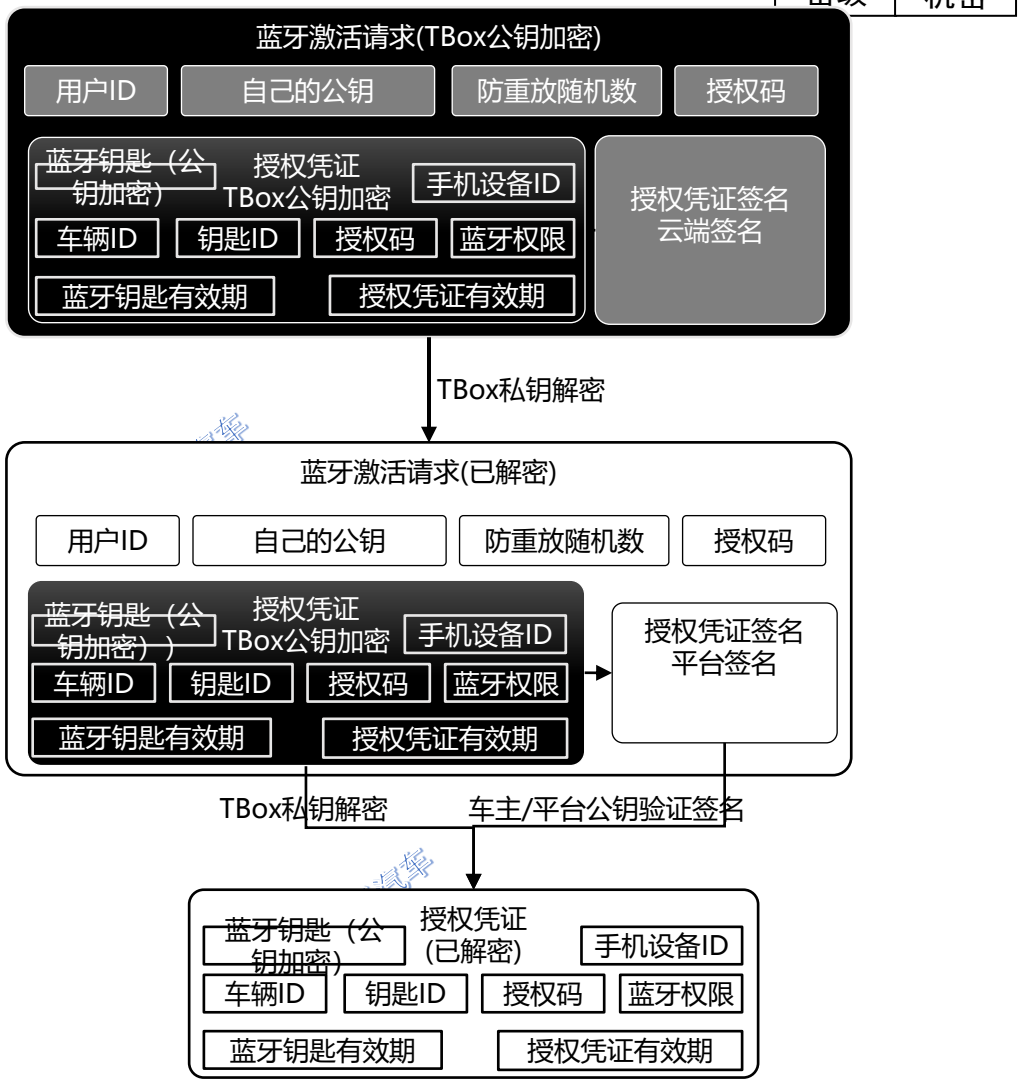
1. 蓝牙授权申请：车辆ID, 被授权人手机号，蓝牙钥匙生效时间，蓝牙钥匙失效时间，授予的权限信息，被授权人用户类型(家人，朋友，其他)
2. 蓝牙授权确认参数: 授权码，用户ID，手机设备ID
3. 蓝牙授权信息：参考后续核心数据对象
4. 被授权人激活蓝牙钥匙指令：参考后续核心数据结构”蓝牙激活请求信息”
5. 蓝牙钥匙云端签名(云端蓝牙服务证书私钥)：采用私钥签名算法ECDSA-256 (授权凭证)

蓝牙钥匙方案

被授权人蓝牙钥匙申请 - 核心数据对象



密级 | 机密



蓝牙钥匙方案

宝能 BAONENG

密级	机密

算法约定

算法名称	算法类型	算法	密钥长度	使用场景
公钥加密	非对称加密	ECC	256	蓝牙钥匙的公钥加密/解密 授权凭证的加密/解密 蓝牙激活请求的加密/解密
私钥签名	非对称签名	ECDSA	256	蓝牙钥匙的签名/验签 授权凭证的签名/验签
对称加密	对称加密	AES	128	蓝牙控制指令加密

蓝牙钥匙方案

宝能 BAONENG

密级	机密

被授权人蓝牙钥匙申请- 蓝牙钥匙激活处理过程

手机App靠近车辆，准备激活蓝牙钥匙

- 用户靠近车辆，点击“激活蓝牙钥匙”
- 手机App验证授权凭证有效期
- 手机App向车辆发起蓝牙连接，获得防重放随机数
  蓝牙连接名，蓝牙连接pin
- 手机App向车辆发起蓝牙授权激活请求（参考蓝牙钥匙激活指令）
  指令参数{用户ID, 移动设备ID，授权码，授权凭证，授权凭证签名(云端签名), 自己的公钥，防重放随机数}
  整个指令数据需要采用TBox公钥加密
- TBox采用自己的私钥解密蓝牙钥匙激活请求参数
- TBox比对防重放随机数和内存中该连接对应的防重放随机数是否一致
- TBox采用云端公钥验证“授权凭证”签名
- TBox采用自己的私钥解密“授权凭证”
- TBox比对凭证中的“授权码”和当前申请人提供的是否一致，并查询本地该授权码是否已经被使用了
- TBox验证授权凭证有效期, 验证凭证中的车辆ID是否是自身的车辆ID
- 如果上述验证都通过，则说明是一个合法的蓝牙钥匙激活请求，在本地保存蓝牙钥匙

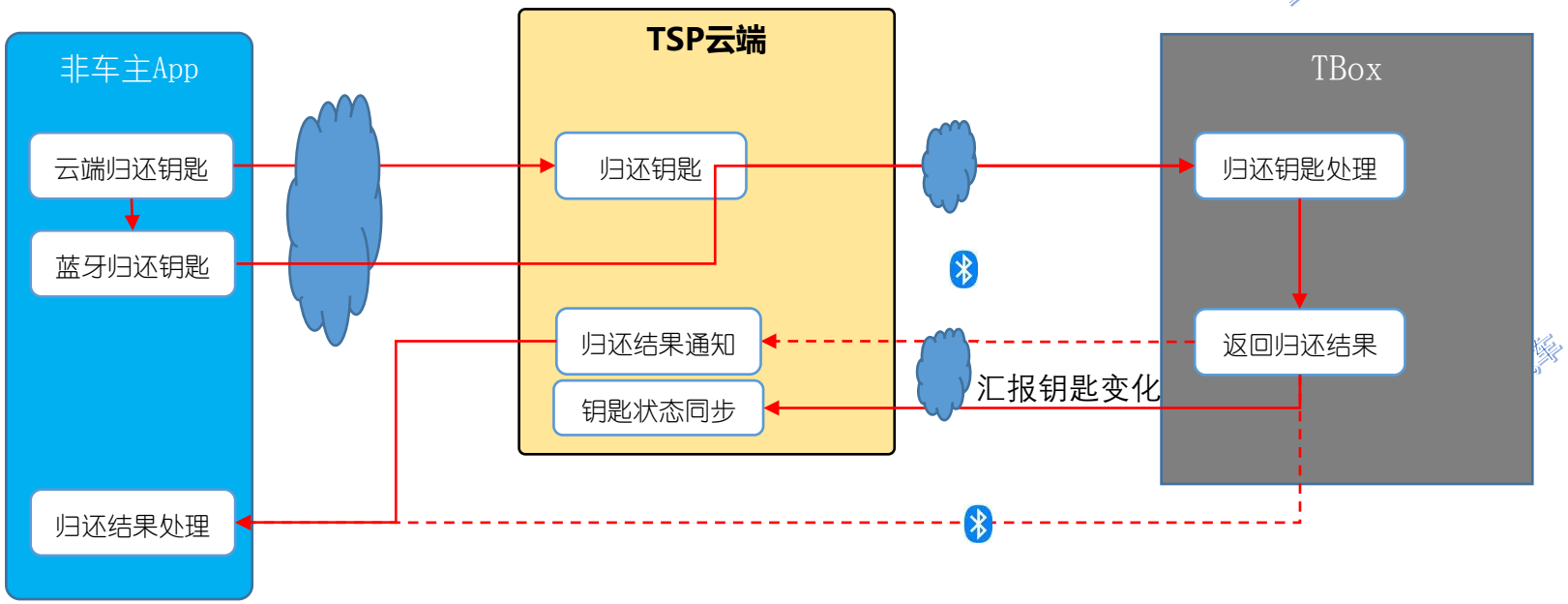
蓝牙钥匙方案

宝能 BAONENG

密级	机密

蓝牙钥匙变更管理

1. 车主的蓝牙钥匙定期主动的更新（后台无感）
2. 车主可以主动的刷新自己的蓝牙钥匙（车主可以看到自己各车的蓝牙钥匙上次更新时间，更新方式，以及有效期等）
3. 车主可以主动收回借出的蓝牙钥匙，由车主通过云端触发蓝牙钥匙的归还，并通知到借车人，在存在本地蓝牙的情况下，归还指令同时通过蓝牙向TBox发出。
4. 非车主可以归还自己借到的车辆蓝牙钥匙, APP首先向云端发起钥匙归还指令，云端将钥匙归还指令转发给TBox, TBox将指令钥匙归还处理，包括检查门窗状态，进行一些自动处理，最后反馈云端归还成功或失败。在存在本地蓝牙的情况下，归还指令同时通过蓝牙向TBox发出。
5. 支持通过蓝牙通道归还蓝牙钥匙
6. 蓝牙钥匙因有效期到，而主动失效，需要由TBox端，云端，手机App端各自管理



蓝牙钥匙方案

宝能 BAONENG

密级	机密

蓝牙钥匙连接信息管理

1. 蓝牙钥匙的连接信息包括：蓝牙连接名称，蓝牙pin码
2. 车主和非车主使用不同的连接pin, 每种连接pin在同一时刻，只能有一个有效的
3. 蓝牙连接名支持修改（由车主主动发起，修改后需要自动通知相关的有效的借车人）
4. 车主的连接pin支持车主手动修改
5. 非车主的连接pin不允许修改，只能作废,重新申请。

蓝牙钥匙方案

宝能 BAONENG

密级	机密

蓝牙钥匙信息存储

1. 手机App端蓝牙钥匙存储（多车多钥匙）：
车辆ID,蓝牙钥匙ID, 蓝牙钥匙（公钥加密），蓝牙钥匙生效时间，蓝牙钥匙失效时间，状态，蓝牙名称，蓝牙连接pin, TBox公钥，蓝牙钥匙云端签名，蓝牙授权清单

2. 云端蓝牙钥匙存储（多人多车多钥匙）：
用户ID, 手机设备ID，车辆ID, TBox ID,蓝牙钥匙ID， 蓝牙钥匙（公钥加密），蓝牙钥匙生效时间，蓝牙钥匙失效时间，状态，蓝牙钥匙云端签名，车主/非车主，蓝牙授权清单等

3. TBox端蓝牙钥匙存储（多人多钥匙）：
蓝牙钥匙ID, 用户ID , 手机设备ID, 蓝牙钥匙（公钥加密），蓝牙钥匙生效时间，蓝牙钥匙失效时间，状态，车主/非车主, 授权码
创建时间，注销时间，创建渠道，注销渠道,
蓝牙钥匙云端签名,
蓝牙授权权限(采用8字节位表达，每一个位代表一个权限)

蓝牙钥匙方案

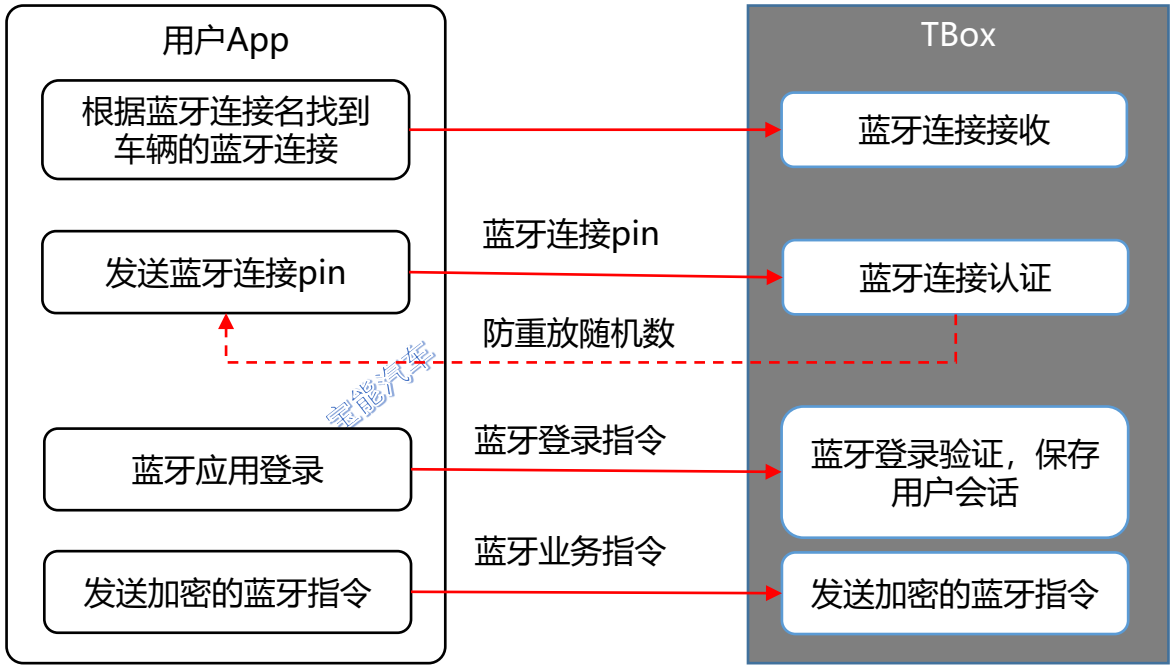
宝能 BAONENG

密级	机密

蓝牙通讯

TBox蓝牙职责
　　建立加密的安全通道（依赖蓝牙芯片）
　　负责实现对连接者的鉴权
蓝牙鉴权机制：
　　TBox蓝牙模块支持SMP协议的
　　　　采用SMP协议完成蓝牙配对和鉴权
　　TBox蓝牙模块不支持SMP协议
　　　　需要和蓝牙模块供应商协商鉴权机制

1. 蓝牙连接
   - ◆ 手机App通过蓝牙连接名找到需要连接的蓝牙
   - ◆ 连接成功后手机App向Tbox发送蓝牙连接pin
   - ◆ TBox蓝牙模块验证蓝牙连接pin是否正确
   - ◆ 如果蓝牙连接pin验证通过，则唤醒TBox
   - ◆ Tbox返回防重放随机数
2. 蓝牙应用登录(参考蓝牙登录指令)
   - ◆ 蓝牙连接成功后3秒内必须发出登录指令
   - ◆ App发送蓝牙登录指令(参考后续蓝牙登录指令格式)
   - ◆ 登录成功后，Tbox将维护该连接通道信息，与用户绑定
3. 蓝牙业务指令发送（参考蓝牙业务指令）
   - ◆ 出于性能的考虑蓝牙指令均采用对称密钥加密
   - ◆ 指令信息：参考指令格式
   - ◆ 加密种子: 防重放随机数+蓝牙密钥+用户ID
   - ◆ 加密算法：采用对称加密算法AES 128位
4. TBox验证手机App发起的蓝牙指令
   - ➢ 根据当前通道找到对应的蓝牙钥匙（有效的）
   - ➢ 采用“防重放随机数+蓝牙密钥+用户ID”作为种子解密消息体
   - ➢ 如果解密失败，则忽略该指令，并中断连接



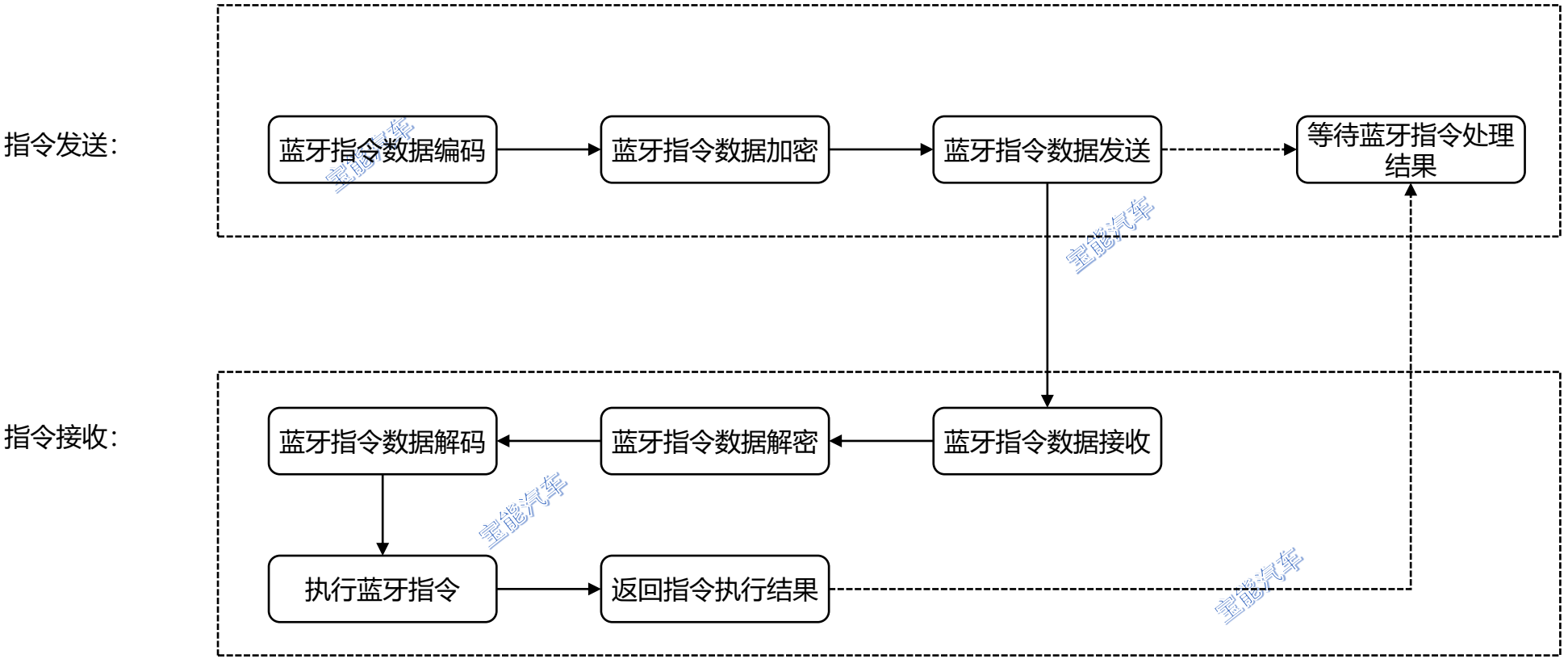
蓝牙连接会话信息：
防重放随机数，用户ID, 移动设备ID，蓝牙钥匙

蓝牙钥匙方案

宝能 BAONENG

密级	机密

蓝牙通讯交互流程



蓝牙钥匙方案

宝能 BAONENG

密级	机密

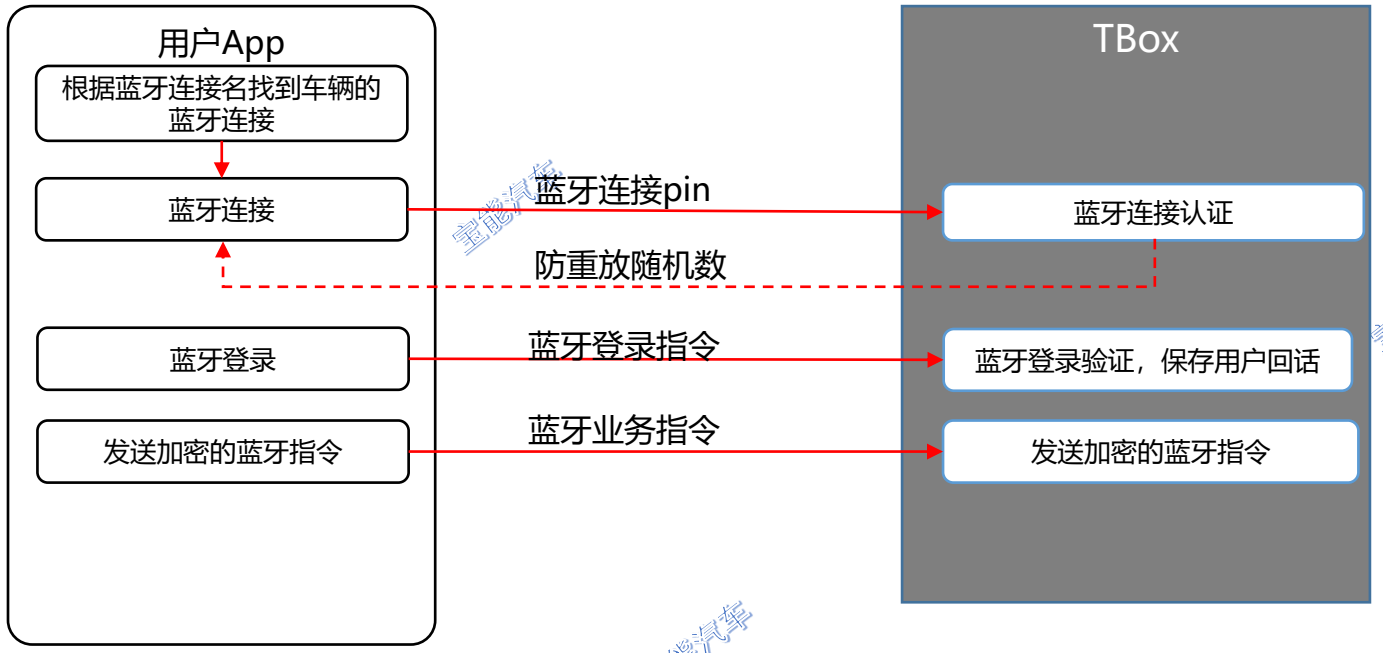
蓝牙通讯指令

1. 蓝牙钥匙激活请求指令包含以下参数

```
{
    指令类型，//1-蓝牙激活,2-登录,3-业务指令
    指令内容(TBox公钥加密)
    {
        参考核心数据”蓝牙激活请求“
    }
}
```

蓝牙钥匙方案

蓝牙通讯指令



蓝牙钥匙对称加密：

加密算法：AES 128

加密种子：防重放随机数+用户ID+蓝牙钥匙

2.蓝牙连接会话信息：

防重放随机数，用户ID, 手机设备ID, 蓝牙钥匙 机密

3. 蓝牙登录指令（蓝牙连接成功后3秒内发起登录指令）：

```
{
        指令类型，//1-蓝牙激活，2-登录，3-业务指令
        用户ID,          //用户ID,建议数值型
        手机设备ID,      //区分在不同的手机设备
        加密的蓝牙指令 //采用蓝牙钥匙对称加密
        {
                用户ID,
                手机设备ID,//区分在不同的手机设备
        }
}
```

4. 蓝牙业务指令：

```
{
    指令类型，//1-蓝牙激活，2-登录, 3-业务指令
    加密的蓝牙指令 //采用蓝牙钥匙对称加密
    {
            指令ID,
            指令,
            指令时间, //UTC时间毫秒数
            指令有效期 //单位:秒
    }
}
```

蓝牙钥匙方案

宝能 BAONENG

密级	机密

蓝牙传输协议-设计的目的

本方案设计旨在解决移动设备App到TBox终端之间的蓝牙通讯问题。

由于低功耗蓝牙钥匙单次数据传输有限，通常在20到几十个字节，而应用程序通常情况下一次需要传输的数据可能超过或远超过次字节数的限制，因此本协议需要实现蓝牙通讯的超长字节数的传输，通过数据的拆包和组包实现超长字节数的传输。

在手机App同TBox进行通讯时，存在针对发出的消息需要等待对方返回值的情景，即消息的同步发送；也存在发出的消息无需等待对方返回结果的情景，本方案要求支持上述两种机制（有返回值的请求和无返回值的请求）。

本方案中要求发送给对方的每一条消息都需要对方给与一个收到确认，否则视为消息错误丢失。

下述方案中提到的字节或数值为特殊说明的均指无符号型数值。

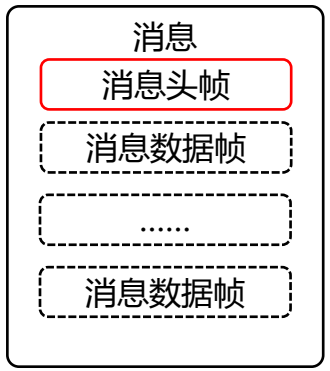
蓝牙钥匙方案

宝能 BAONENG

密级	机密

蓝牙传输协议-协议结构

- 通过蓝牙传输的消息，由于蓝牙单次传输数据有限(比如20)，一条消息通常需要拆分为多帧传输
- 本方案约定蓝牙芯片单次最大传输的字节数为n （MTU大小，比如20）
- 每一条消息将包含至少1个**消息头帧**，0个或多个**消息数据帧**



蓝牙钥匙方案

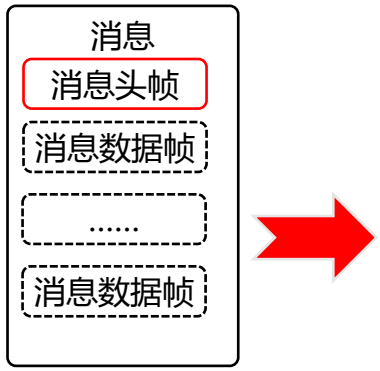
宝能 BAONENG

密级	机密

蓝牙传输协议-消息头帧定义

消息头帧

- 在消息头中可以携带部分消息数据。
- 消息头帧按消息类型分为**请求消息头**和**响应消息头**两种类型，他们在第一字节的4-3位有所差异。
  - **请求消息**指主动向对方发送消息使用的帧，其包含请求头帧和数据帧两部分
  - **响应消息**指针对对方的请求，给出一个响应消息，在请求方要求响应时才会产生和返回此响应帧。



字段	字节数	位	说明	
帧标识	1	7-6	消息类型 0 – 请求 1 – 响应	如果是主动向对方发消息，则类型设置为0 如果是对对方消息的响应，则类型设置为1
		5	分帧类型 0 – 单帧 1 – 多帧	如果业务数据可以直接通过头帧剩余的空间传输，则分帧类型设置为0，否则设置为1
		4-3	是否需要响应(消息类型=0) 0 – 不需要 1 – 需要 响应类型(消息类型=1) 0 –消息帧丢失，需重传 1 –消息接收失败 2 –消息帧全部收到 3 –业务消息响应	整个消息完全接收成功或者失败必须给发送方一个接收结果的响应； 此处的“是否响应”是指消息接收方是否需要给对方一个业务上的响应结果（调用返回值）
		2-1	保留，默认0	
总帧数	1	7-0	单帧：1 多帧：2-255	总帧数采用一个无符号字节表达，最大支持255帧 包含头帧和数据帧
数据长度	1	7-0	最大值：n-3	指当前帧的实际数据长度，头帧可最大携带n-3个字节
消息数据	0 ~ (n-3)		最大字节数：n-3	

蓝牙钥匙方案

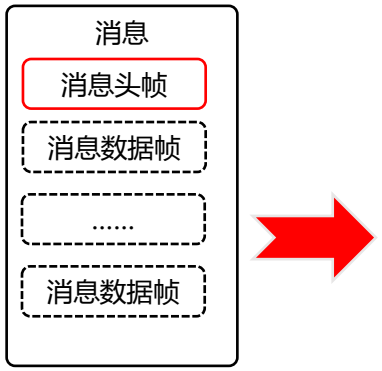
宝能 BAONENG

密级	机密

蓝牙传输协议-消息数据帧

数据帧

数据帧用于在多帧传输中，用于描述和携带需要传输的数据。



字段	字节数	位	说明
帧标识	1	7-6	帧类型 2 – 数据帧
		5	是否最后一帧 0 – 否 1 – 是
		4	保留，默认0
		3	保留，默认0
		2	保留，默认0
		1	保留，默认0
当前帧序号	1		1-255
数据长度	1		最大值：n-3
数据体	0 ~ (n-3)		最大字节数：n-3

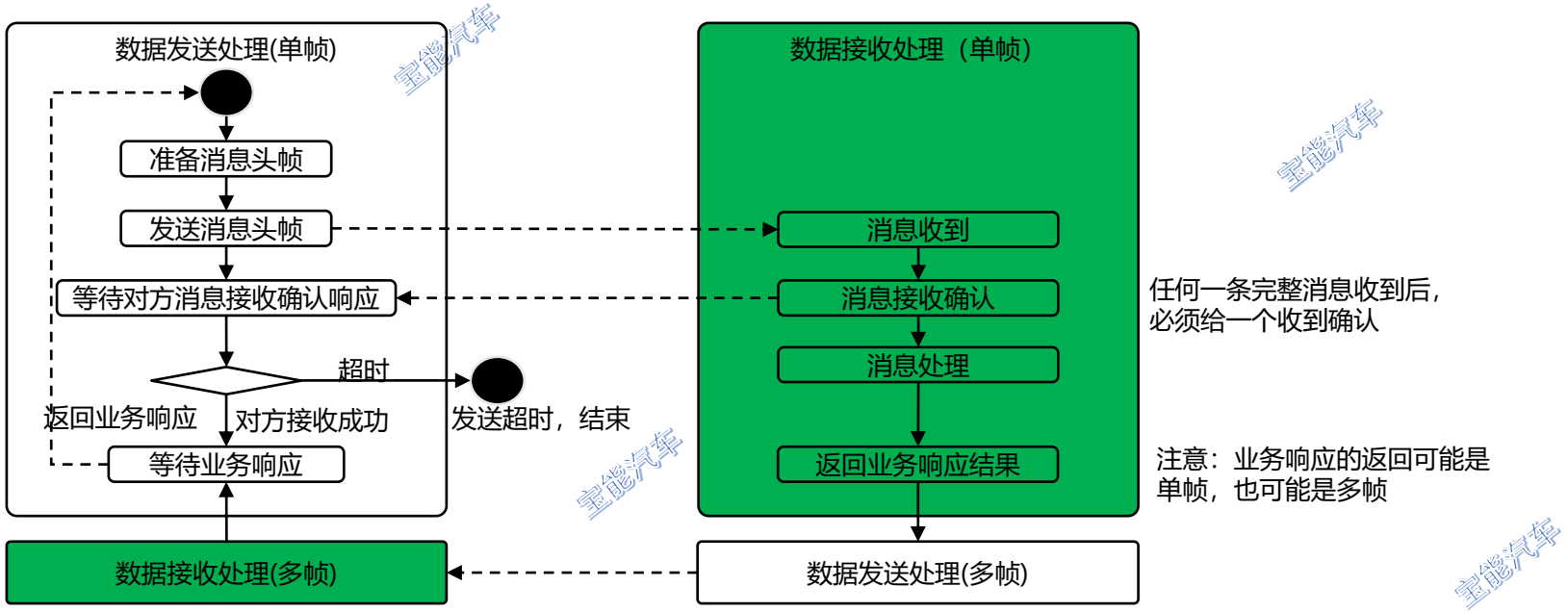
蓝牙钥匙方案

宝能 BAONENG

密级	机密

蓝牙传输协议-单帧传输

定义：单帧传输是指需要传输的蓝牙数据可以在一次蓝牙传输中完成的数据传输方式
前提条件：数据长度<n-3,” n”指蓝牙支持的MTU大小，比如n=20,则每次传输的数据必须<=n-3(17个字节)
适应范围：请求指令和指令响应均可以采用单帧传输模式，采用何种方式取决于需要传输的数据的大小



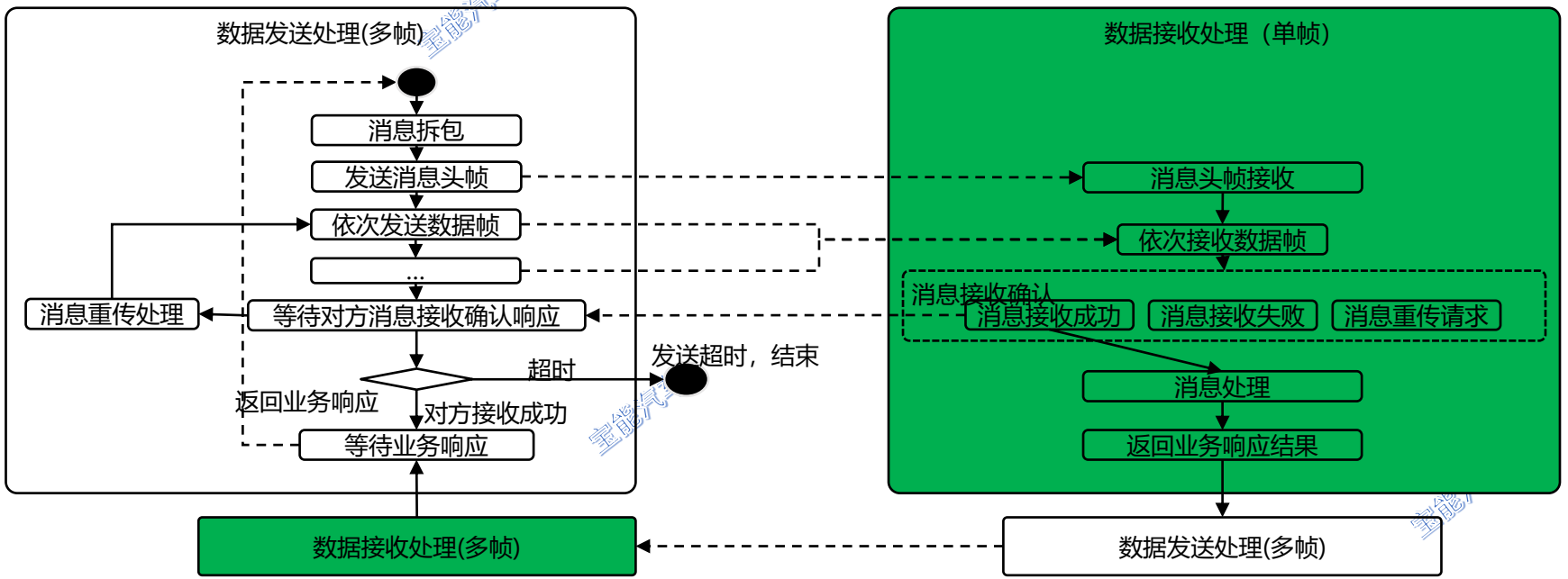
蓝牙钥匙方案

宝能 BAONENG

密级	机密

蓝牙传输协议-多帧传输

定义：多帧传输是指需要传输的蓝牙数据因为太大需要分为多次发送给对方
前提条件：数据长度>n-3,” n” 指蓝牙支持的MTU大小，比如n=20,则每次传输的数据>n-3(17个字节)
适应范围：请求指令和指令响应均可以采用多帧传输模式，采用何种方式取决于需要传输的数据的大小
传输大小：(255-1)*(n=3), 比如n=20, 则允许发送的消息大小:4318个字节



消息错误处理

消息接收方在收到最后一帧时，断定对方已发送消息结束，如果在一定的时间内仍未得到最后一帧，断定对方消息发送失败。

当帧的丢失率<10%时，可以要求发送方重新传输丢失的帧，数据体中存放丢失帧的序号，一个字节一个序号。

如果丢失率>10,则直接响应消息宣告数据传输失败。

任何一条完整消息收到后，必须给一个收到确认

注意：业务响应的返回可能是单帧，也可能是多帧

蓝牙钥匙方案

宝能 BAONENG

密级	机密

蓝牙数据协议

蓝牙数据协议旨在定义业务数据通过蓝牙通道进行交互时，数据的打包封装方式，机制或格式，该协议的目的是需要提供一种通用的封装方式，可以考虑采用自定义二进制格式，json, pb或TLV等。Json,pd协议在特定的环境下难以支撑，而TLV协议相对简洁，因此本方案将考虑采用TLV作为数据打包封装方案。

蓝牙钥匙方案

宝能 BAONENG

密级	机密

服务与接口设计

服务发起方	服务提供方	接口机制/协议
手机App	TSP后台	API
TBox	TSP后台	MQTT协议
手机App	TBox	

蓝牙钥匙方案

宝能 BAONENG

密级	机密

服务与接口设计

TSP后台服务

服务分类	模块	服务名称	参数	响应	使用者	说明
面向手机App的服务	车主蓝牙钥匙申请	蓝牙钥匙申请	车辆Id 手机设备ID	蓝牙钥匙	车主	提供给车主申请蓝牙钥匙 返回采用个人公钥加密的蓝牙钥匙
		关闭蓝牙钥匙服务			车主	车主关闭蓝牙钥匙服务
		获取已申请的蓝牙钥匙	车辆Id 手机设备ID	车辆ID 蓝牙钥匙	所有App用户	在更换手机的场景下恢复蓝牙钥匙 获取指定车辆或者所有已申请的蓝牙钥匙记录
	蓝牙配置	更新蓝牙配置	车辆Id 蓝牙连接名 蓝牙连接pin	成功/失败	车主	更新蓝牙钥匙连接pin和蓝牙连接名 更新后需要通知所欲相关的蓝牙钥匙使用者
		获取蓝牙配置	车辆Id	蓝牙连接名 蓝牙连接pin	所有App用户	获取其蓝牙钥匙最新的蓝牙配置信息 在蓝牙钥匙有效的情况下才能获取
	蓝牙授权	蓝牙授权申请	车辆ID 授权有效期 授予的角色权限		车主	车主为被授权申请蓝牙授权申请
		蓝牙授权管理			车主	管理自己发出的蓝牙钥匙授权，包括取消蓝牙钥匙授权，修改蓝牙钥匙授权，修改蓝牙钥匙授予的角色等
		我的蓝牙授权	车辆Id		车主	获取车辆授权出去的蓝牙钥匙
		获取授权信息	手机号	授权人 授权的车辆 授权有效期等	被授权人	被授权人收到通知后凭借手机号获取授权信息
		蓝牙授权确认	用户ID 授权码 手机设备ID	蓝牙钥匙授权凭证信息等	被授权人	蓝牙钥匙授权确认，获得蓝牙钥匙授权凭证以及其他相关的授权信息
		我被授权的蓝牙钥匙			所有App用户	获取当前用户被授权的蓝牙钥匙

蓝牙钥匙方案

宝能 BAONENG

密级	机密

服务与接口设计

TSP后台服务

服务分类	模块	服务名称	参数	响应	使用者	说明
面向手机App的服务	蓝牙钥匙管理	蓝牙钥匙有效期修改	车辆Id， 新的过期时间 蓝牙钥匙ID	成功/失败	车主	车主修改蓝牙钥匙的过期时间 主要是修改授权给他人的蓝牙钥匙的有效期
		蓝牙钥匙更换	车辆Id 移动设备ID	新的蓝牙钥匙	车主	用车人更新自己的蓝牙钥匙
		蓝牙钥匙注销	车辆Id 蓝牙钥匙ID	成功/失败	所有App用户	车主注销已授权的蓝牙钥匙 非车主归还车辆注销蓝牙钥匙
	日志	上传访问日志	访问日志	成功/失败	所有App用户	

蓝牙钥匙方案

宝能 BAONENG

密级	机密

服务与接口设计

TSP后台服务

服务分类	方向	服务名称	参数	响应	使用者	说明
TBox服务	下行	蓝牙钥匙申请	用户ID 手机设备ID 密钥过期时间 车主公钥	蓝牙钥匙 蓝牙连接名称 蓝牙连接pin	TSP后台	采用用户公钥加密的蓝牙钥匙
	下行	更新蓝牙钥匙配置	蓝牙连接名 蓝牙连接pin	成功/失败	TSP后台	
	下行	获取蓝牙钥匙配置	无	蓝牙连接名 蓝牙连接pin	TSP后台	
	下行	蓝牙钥匙有效期修改	用户ID 手机设备ID 密钥过期时间	成功/失败	TSP后台	
	下行	蓝牙钥匙更换	用户ID 手机设备ID	蓝牙钥匙	TSP后台	采用用户公钥加密的蓝牙钥匙
	下行	蓝牙钥匙注销	用户ID 手机设备ID	成功/失败	TSP后台	
	上行	上传访问日志	用户ID 日志信息	成功/失败	TSP后台	

蓝牙钥匙方案

宝能 BAONENG

密级	机密

服务与接口设计

手机App功能

通讯对象	服务名称	参数	响应	使用者	说明
TSP后台	蓝牙钥匙申请			车主	
	获取已申请的蓝牙钥匙			所有App用户	
	更新蓝牙配置			车主	
	获取蓝牙配置			所有App用户	
	申请蓝牙授权凭证			车主	
	蓝牙授权确认			非车主	
	蓝牙钥匙有效期修改			车主	
	蓝牙钥匙更换			所有App用户	
	蓝牙钥匙注销			所有App用户	
	接收蓝牙连接信息更新通知			App后台	
	上传访问日志			App后台	

蓝牙钥匙方案

宝能 BAONENG

密级	机密

服务与接口设计

手机App功能

服务分类	服务名称	参数	响应	使用者	说明
TBox	连接TBox蓝牙	蓝牙连接名 蓝牙连接pin	防重放随机数	App后台	
	激活蓝牙钥匙	参考方案	参考方案	非车主	
	...其他蓝牙指令				