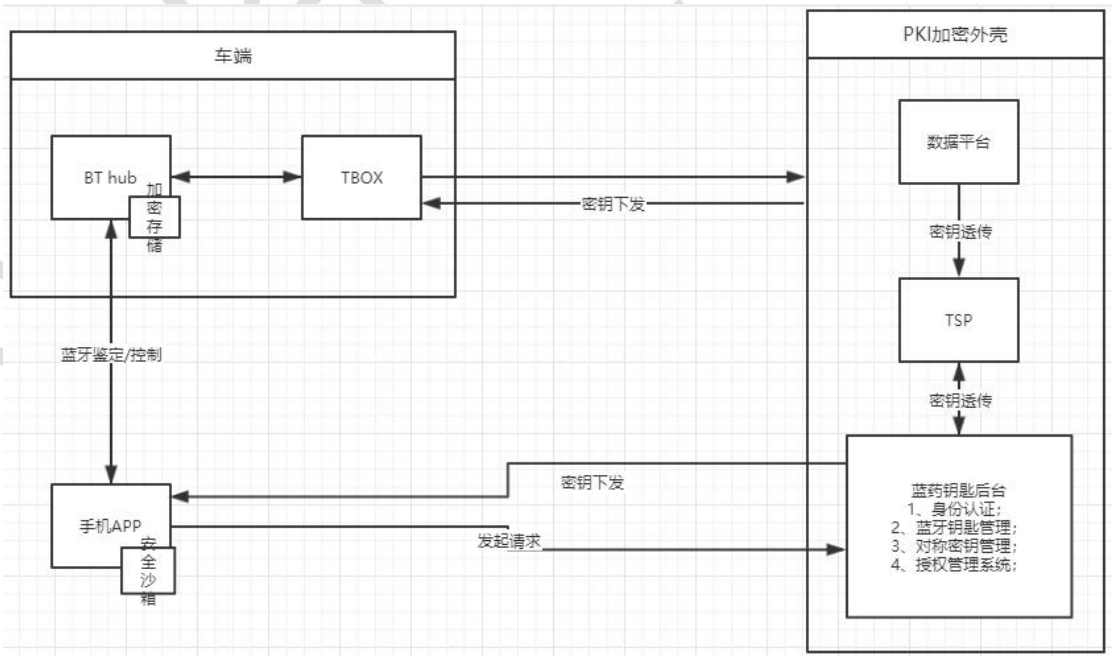
GX16 蓝牙钥匙产品设计文档

修改记录			
序号	姓名	日志	日期
1	何思敏	Create	2020-3-2
2			

1. 产品概述

用户绑定车辆成功后，在 云平台会自动为其生成蓝牙钥匙，通过蓝牙钥匙可实现 APP 端车门上锁/车门解锁/开启后备箱/启动车辆功能。车主也可以在 APP 授权蓝牙钥匙给其他用户，获得授权的用户可以通过远程控制实现无钥匙驾驶车辆，蓝牙钥匙具有时效性，超过时效无法使用。

2. 功能架构



蓝牙钥匙产品架构图

FeatureList

Main Features	Subfunctions	Description
蓝牙钥匙预置	预置蓝牙钥匙	车辆下线时车载端蓝牙钥匙预置到 BT HUB 加密存储模块
蓝牙钥匙申请	车主申请蓝牙钥匙	车主绑车成功后，将预置的蓝牙钥匙对应的应用端蓝牙钥匙下发到手机 APP
蓝牙钥匙使用	授权人申请蓝牙钥匙	车主授权蓝牙钥匙给被授权人，平台将蓝牙钥匙分别发送至车端和被授权人手机
	被授权人申请蓝牙钥匙	蓝牙鉴权通过后通过手机 APP 控制车门解闭锁，启动发动机（手动）
蓝牙钥匙管理	蓝牙钥匙申请管理	平台处理手机端、车端申请蓝牙钥匙的请求
	蓝牙钥匙授权管理	车主将蓝牙钥匙授权给被授权人，通过平台进行管理
	蓝牙钥匙更新管理	蓝牙钥匙更新策略和更新机制
蓝牙钥匙销毁	蓝牙钥匙到期	使用蓝牙钥匙需要建立蓝牙连接
	手机遗失被盗等作废	通过平台主动作废蓝牙钥匙

3. 数字钥匙模块需求

1） 数字钥匙业务平台

① 能够通过 TSP 接口对 TSP 系统中的用户注册信息进行查询和调用；
② 能够实现数字钥匙申请、生产、分享、授权、下载、更新、注销（包括车主注销、管理员后台注销、被分享者主动归还注销）等相关操作；
③ 实现数字钥匙的查询、状态追踪、分发记录配套的管理服务；
④ 建立服务器与手机 APP、服务器与安全芯片（或安全存储）的安全加密通道；
⑤ 安全服务需要与 PKI 系统进行对接；
⑥ 能够保存客户的操作指令与个人用户数据的对应关系到安全芯片（或安全存储管理）；
⑦ 数字钥匙下发时应对应蓝牙 MAC、UUID、配对码等车辆特征信息；
⑧ 配合 APP 客户端进行 APP 应用个人化、通信证书个人化、进行业务秘钥安全传输；
⑨ 个人化 APP 侧业务 SDK 和后台建立安全通道的通讯证书；
⑩ 保护数字钥匙运行安全，记录并追踪可能的安全风险和轨迹；

2） PKI 或其它密钥管理平台管理平台

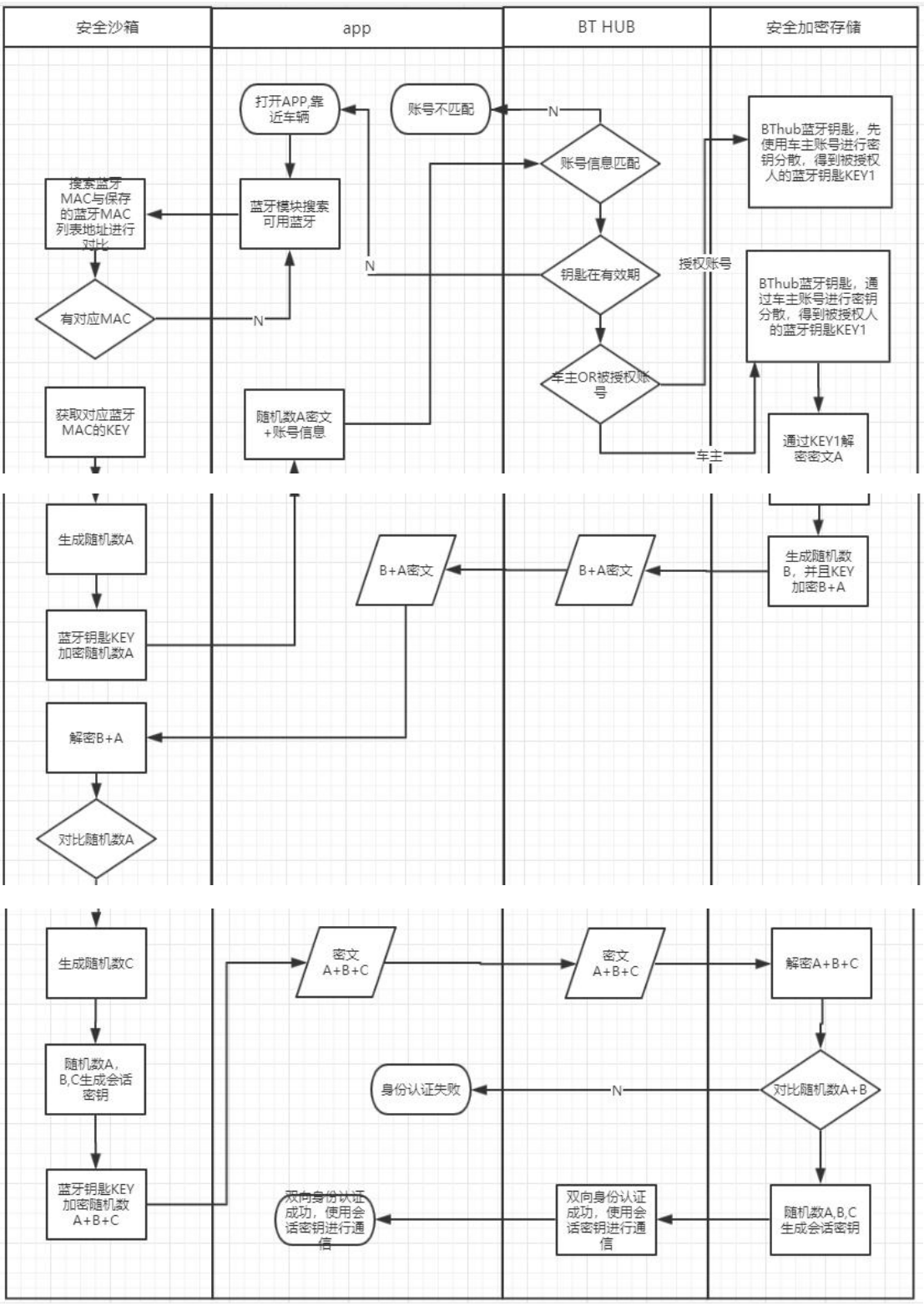
① 更新安全芯片（安全存储）的数字钥匙业务秘钥、机密数据、PKI 证书；
② 下载和更新应用、提供应用管理服务；

3） 手机数字钥匙 SDK

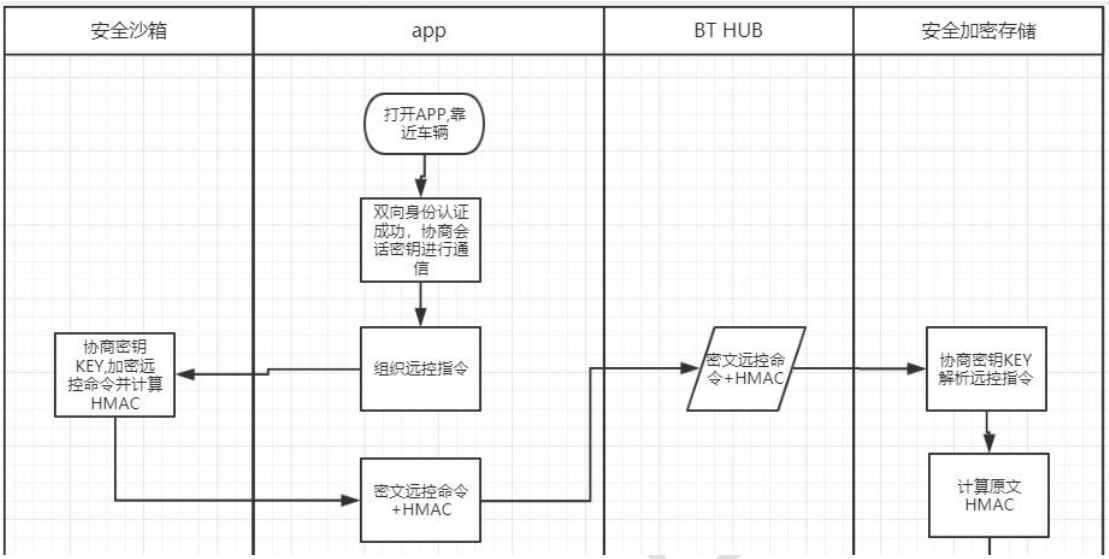
① 能够安全存储数字钥匙、秘钥、证书、客户需求的机密数据；
② 为手机客户端提供对称、非对称白盒密码运算安全服务；
③ 提取手机设备指纹，配置配合 APP 安全管理平台进行个人化管理；
④ 检测设备运行环境，保护数字钥匙运行安全；
⑤ 建立 APP 到服务器的安全通道，APP 到 BT HUB 安全芯片（安全存储）的 BLE 安全加密通道；
⑥ 支持安卓、ios 主流操作系统，及主流机型不少于 100 款；
⑦ 实现钥匙申请、分享、授权、验证、使用及注销（包括车主注销，分享者规划）业务流程；
⑧ 提供接口接收权限次数扣减指令，进行钥匙权限次数扣减；
⑨ 数字钥匙下发时，应下发蓝牙 MAC、UUID、配对码等车辆信息；
⑩ 提供接口，接收 APK 上层通知的蓝牙断开，清楚钥匙相关会化的安全信息；
⑪ 提供专用接口使用会话密钥双向（移动设备和车辆间）；
⑫ 其他加解密传输自定义的配置数据，需要提供数据透传通道；

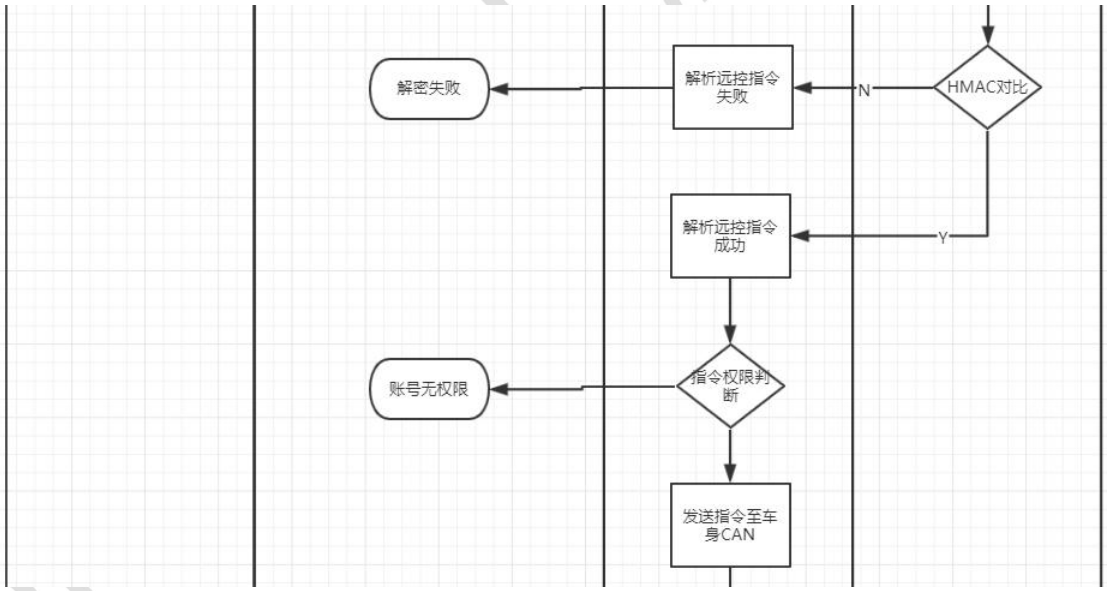
4. 蓝牙钥匙近场链接

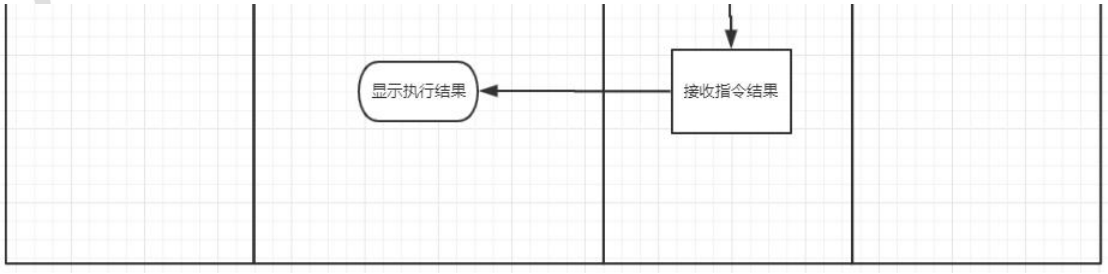
APP 获取 BT HUB 蓝牙的 MAC 地址，与安全沙箱 SSE 中的蓝牙 MAC 进行对比连接连接成功后，BT HUB 和 APP 使用对于加密的蓝牙钥匙进行双向身份认证，并协商生成会话密钥，蓝牙近场控制命令通过会话密钥进行加密保护，每次会话密钥都不一样。



蓝牙钥匙近场链接-近场身份认证



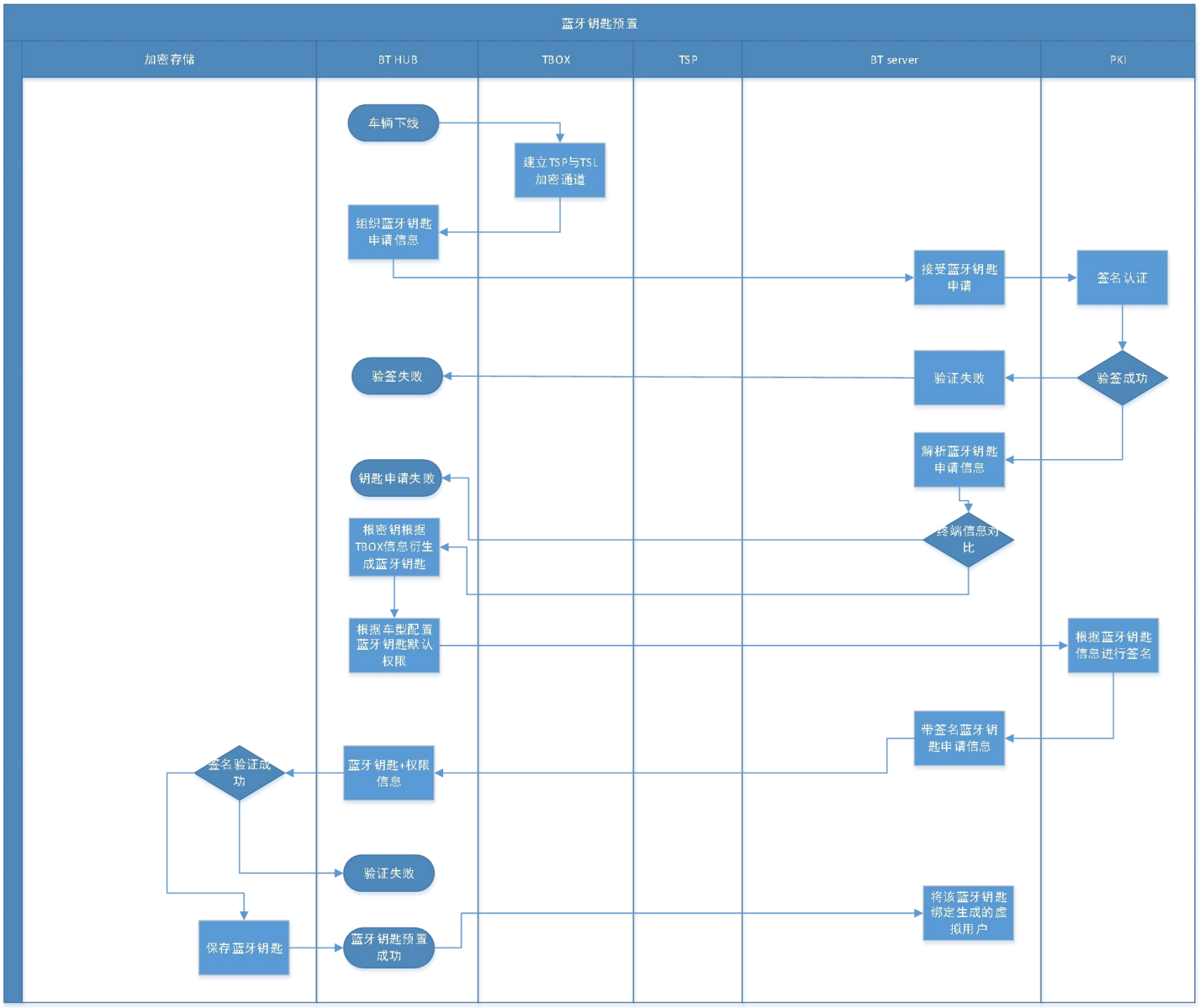




蓝牙钥匙近场链接-蓝牙钥匙控制指令

5. 蓝牙钥匙预置

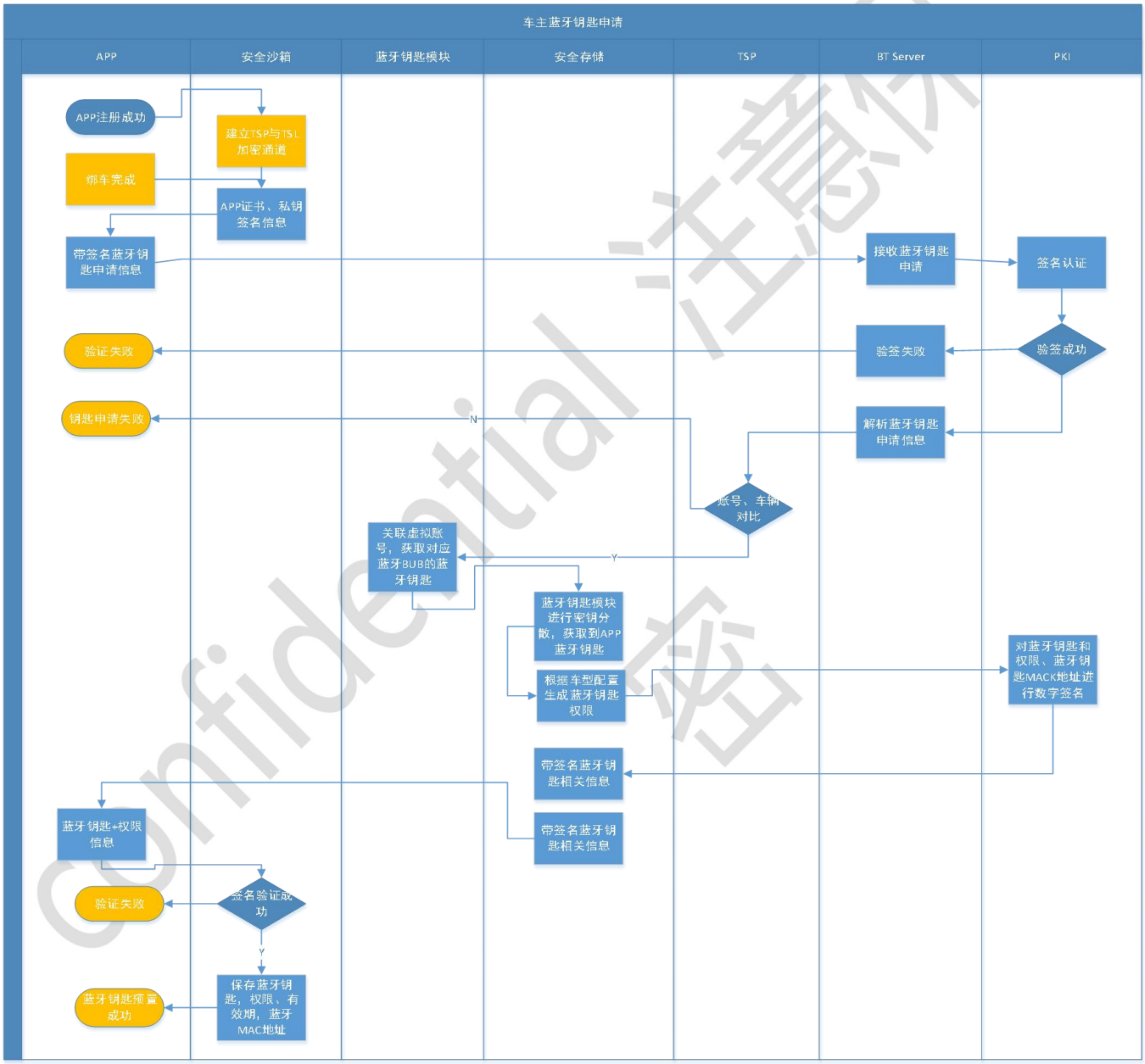
蓝牙钥匙模块根密钥依据车端信息(SN，CCID 等信息)密钥分散获取。车辆下线时，MES 系统调用接口通过 TLS1.2 加密通道连接 TSP 蓝牙钥匙服务，申请获取到蓝牙钥匙。并将蓝牙钥匙保存到加密存储中。每个终端拥有不同的蓝牙钥匙



6. 车主蓝牙钥匙申请

注册成功并且 APP 证书下发后，绑车完成后 TSP 平台将对应车辆预置的蓝牙钥匙的虚拟账号自动关联用户账号， 蓝牙模块根据申请信息匹配到相应终端的蓝牙钥匙，并对终端蓝牙钥匙进行密钥分散，获取到 APP 端蓝牙钥匙并将钥匙发送给手机 APP。

APP 端将蓝牙钥匙保存到 SSE 安全沙箱中。每个 APP 终端使用不同的蓝牙钥匙



7. 蓝牙钥匙分享

蓝牙钥匙有数量限制，同一辆车同一时间最多存在 3 把蓝牙钥匙（包括车主本人的蓝牙钥匙，即之多再分享两把）蓝牙钥匙模块对蓝牙钥匙先用车主账号信息分散再使用被授权人账号进行分散，获取得到被授权人的蓝牙钥匙；