Date Location @qualcomm

Qualcomm

车用数字钥匙系统标准现状

Jiangsheng WANG
Qualcomm

CCC数字车钥匙系统架构

Car Connectivity Consortium ® (CCC)

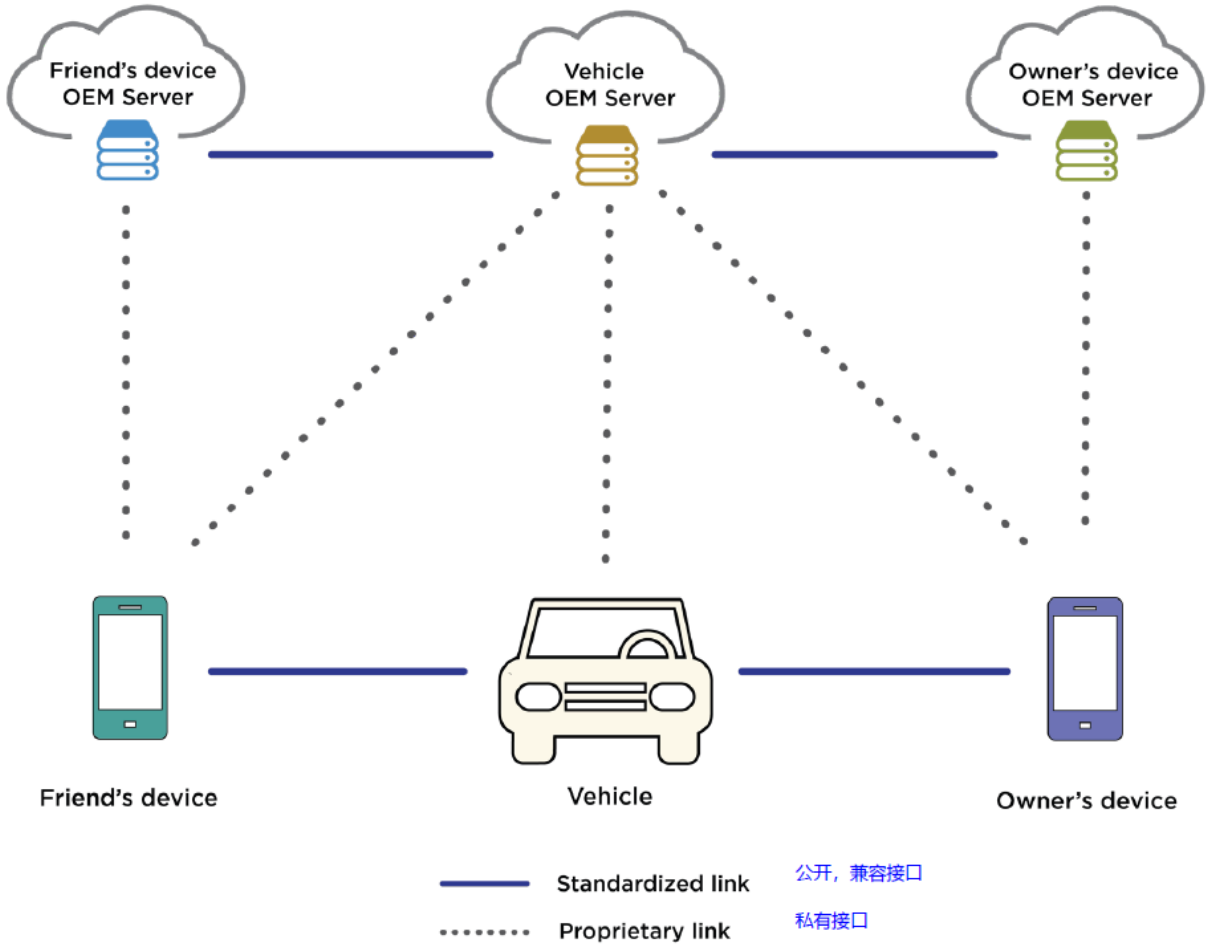


Figure 1: Digital Key System Architecture

The CCC is a cross-industry standards organization with a mission to create sustainable and flexible ecosystems that standardize interface technologies to provide consistently great user experiences across all vehicles and mobile devices.

* CCC-TS-092 **Car Connectivity Consortium Digital Key Technical Specification**

CCC数字车钥匙移动终端侧系统架构

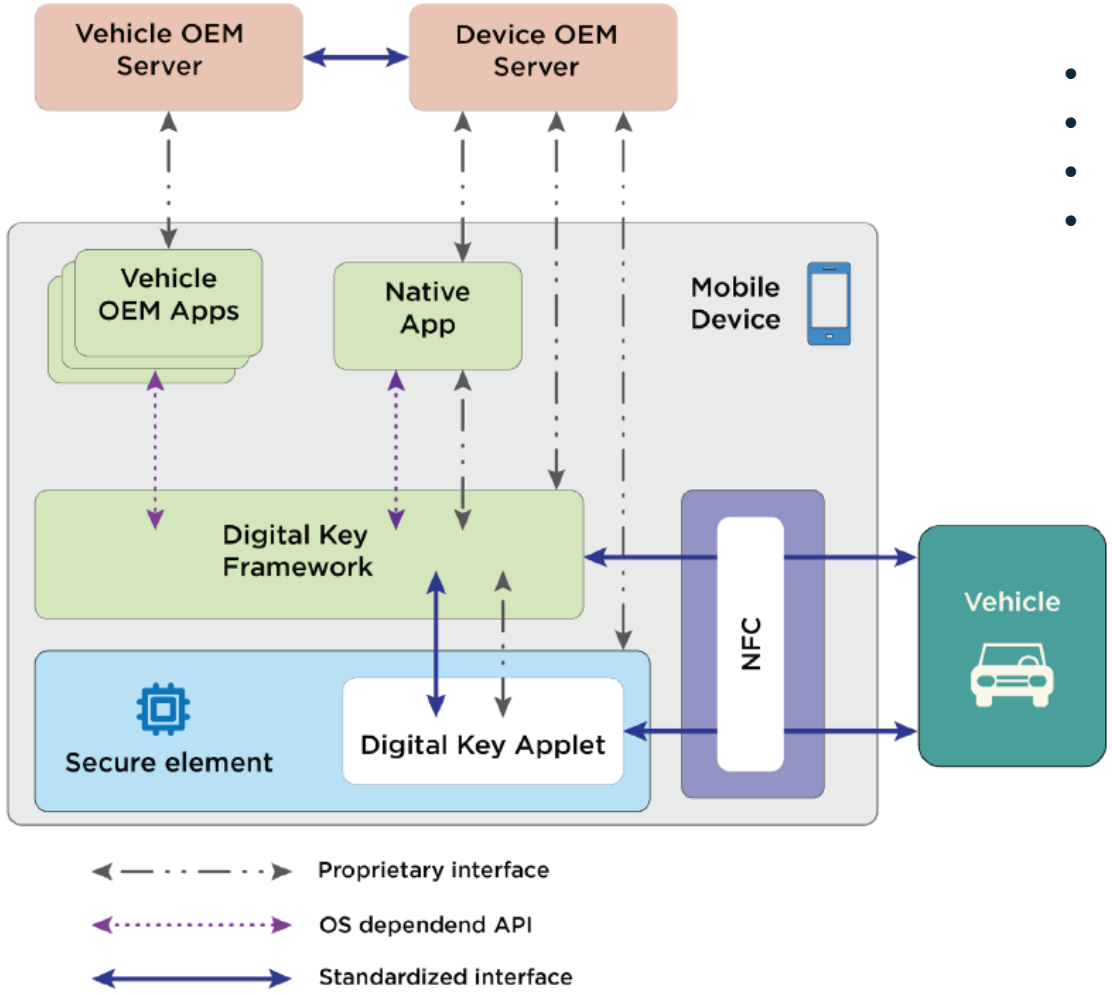


Figure 2: Mobile Device Architecture

- V2.0支持NFC
- V3.0将支持蓝牙，UWB，增加位置（临近关系）检测。
- 重点描述“公开接口”和流程。
- v2.0保留key格式由厂家自行决定

IFFAA数字车钥匙系统架构

互联网金融身份认证联盟“International Internet Finance Authentication Alliance”（英文简称“IIFAA”），成立于2015年，由中国信息通信研究院、蚂蚁金服、华为、三星、阿里巴巴、中兴6家单位联合发起。

工作组

本地免密工作组
数字车钥匙焦点组
物联网安全工作组
远程认证（声纹识别）工作组
测试认证工作组
远程认证（人脸识别）工作组
终端安全工作组

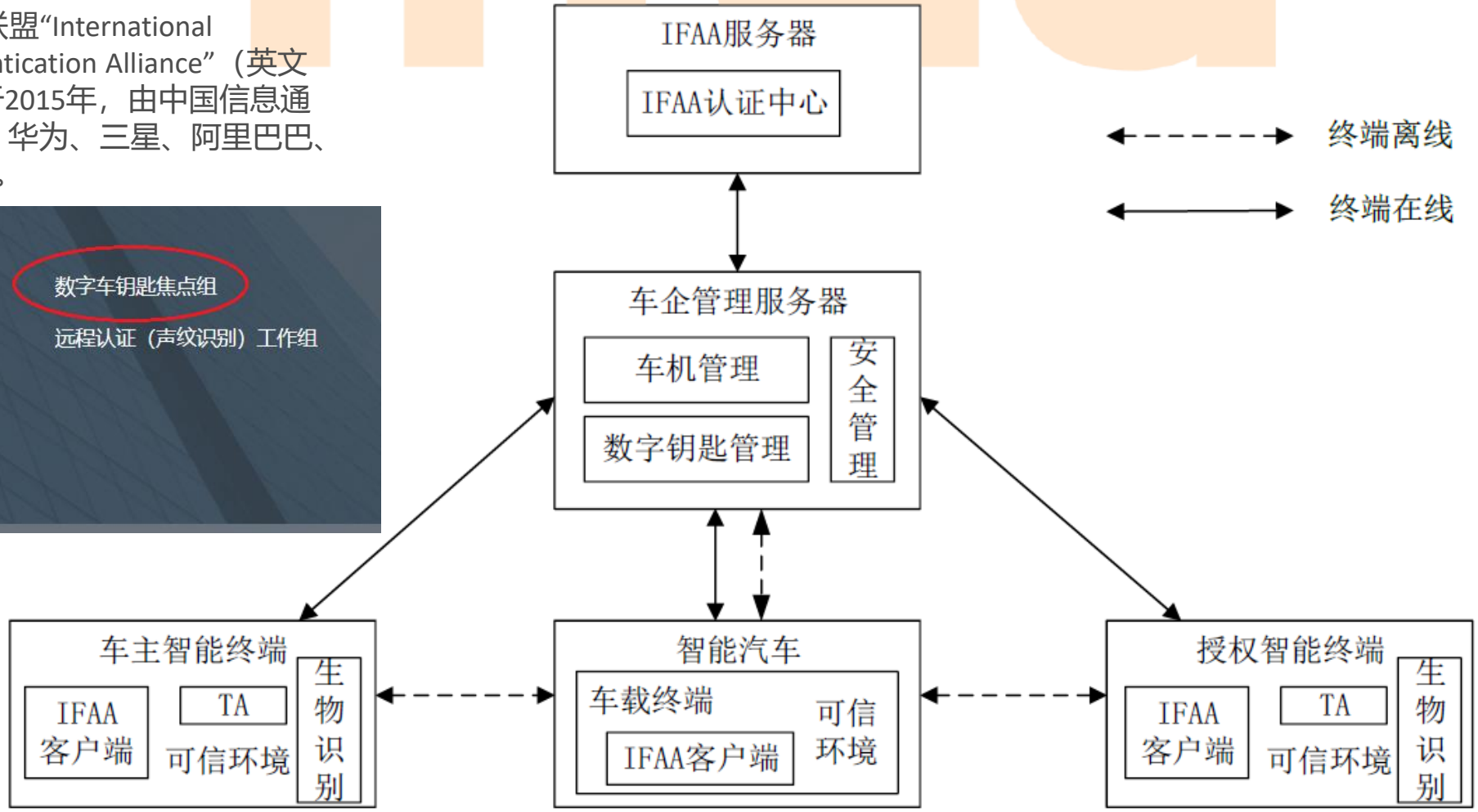
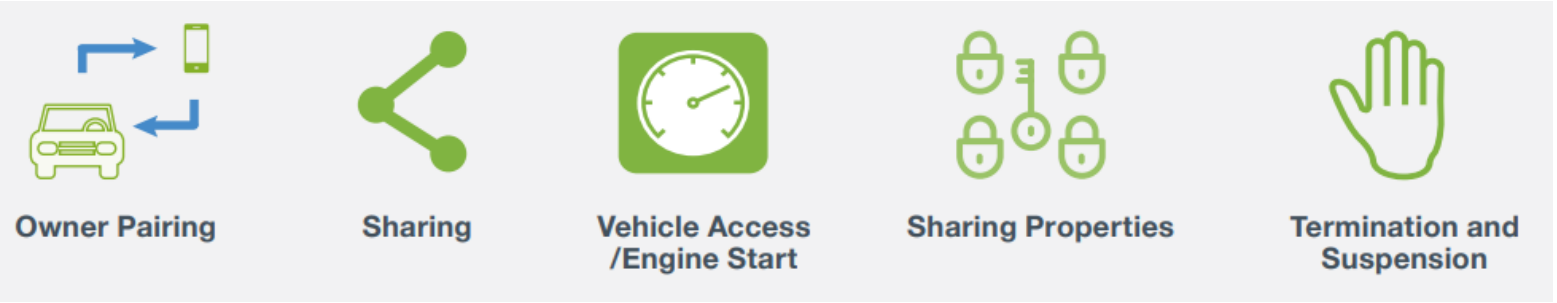


图1　IFAA 数字车钥匙系统总体框架

核心功能与流程

- 核心功能
  - 钥匙管理
  - 钥匙控制操作
- 场景与角色
  - 车主
  - 授权
- 主要管理流程
  - 车钥匙业务管理：设备验证、应用部署、功能开关
  - 车主终端与车配对
  - 钥匙的生成，更新，撤销
  - 车主授权



服务部署流程（CCC v1.0示例）

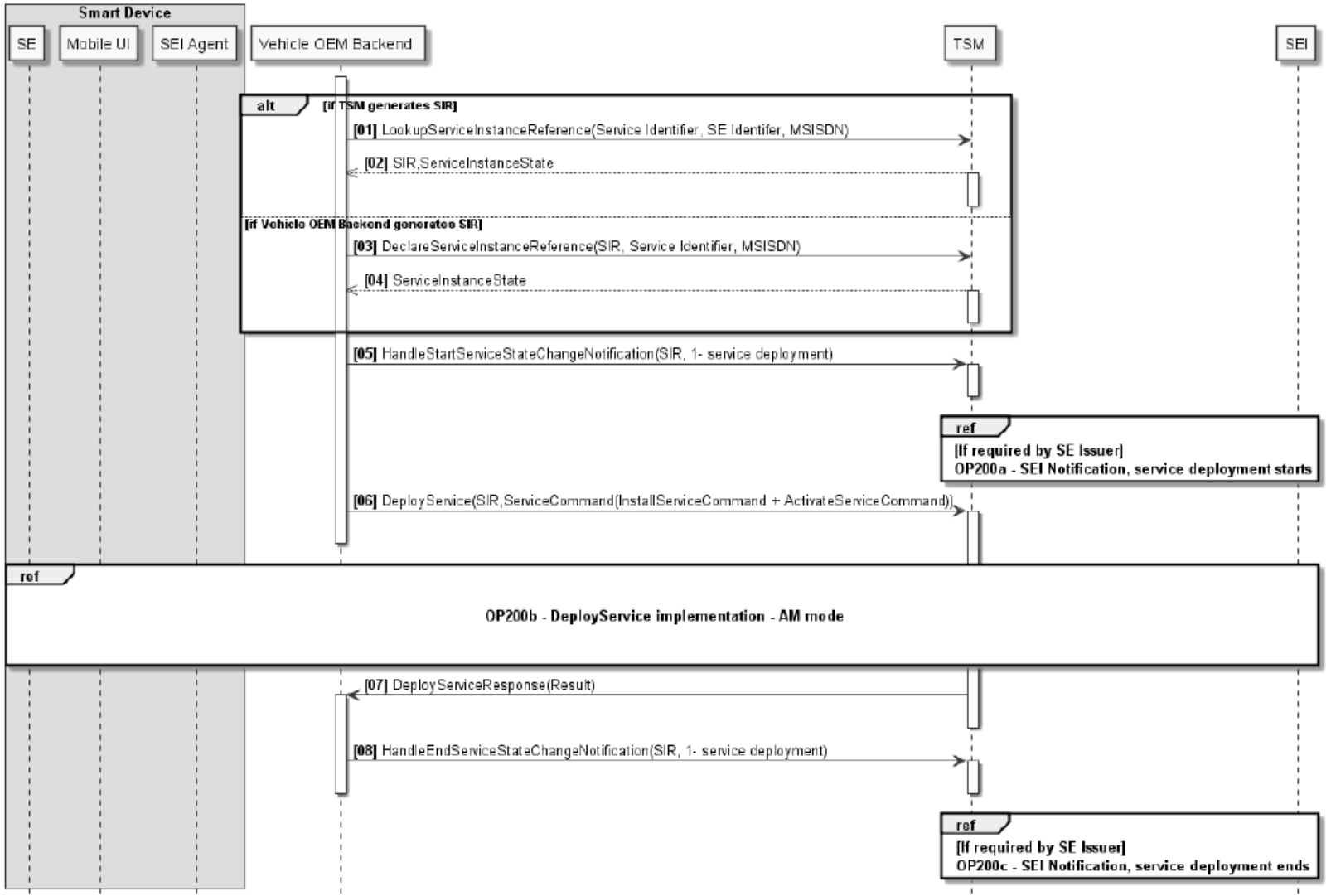


Figure 4-2: OP200 – Service Deployment Procedure

服务部署流程（CCC v1.0示例）

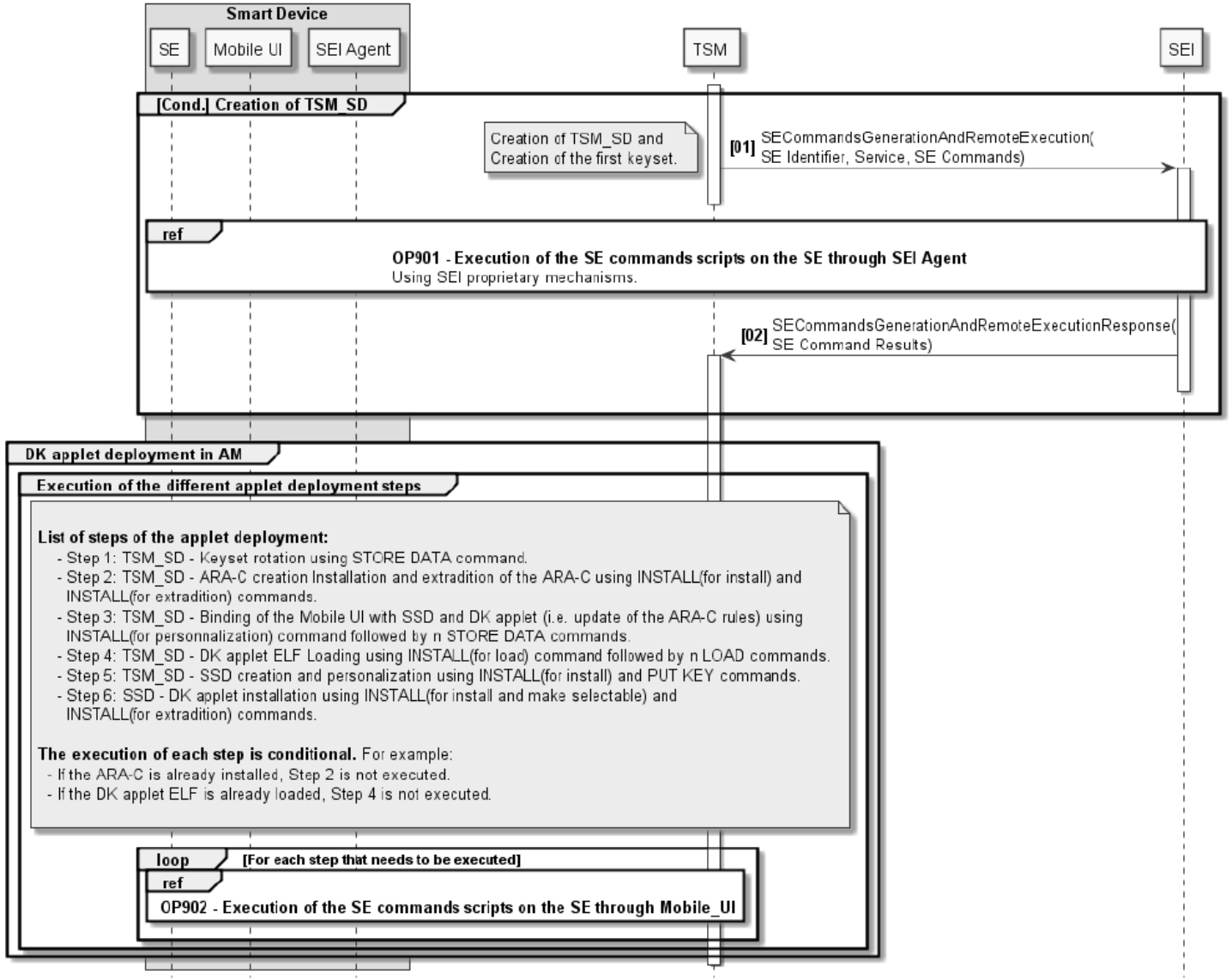
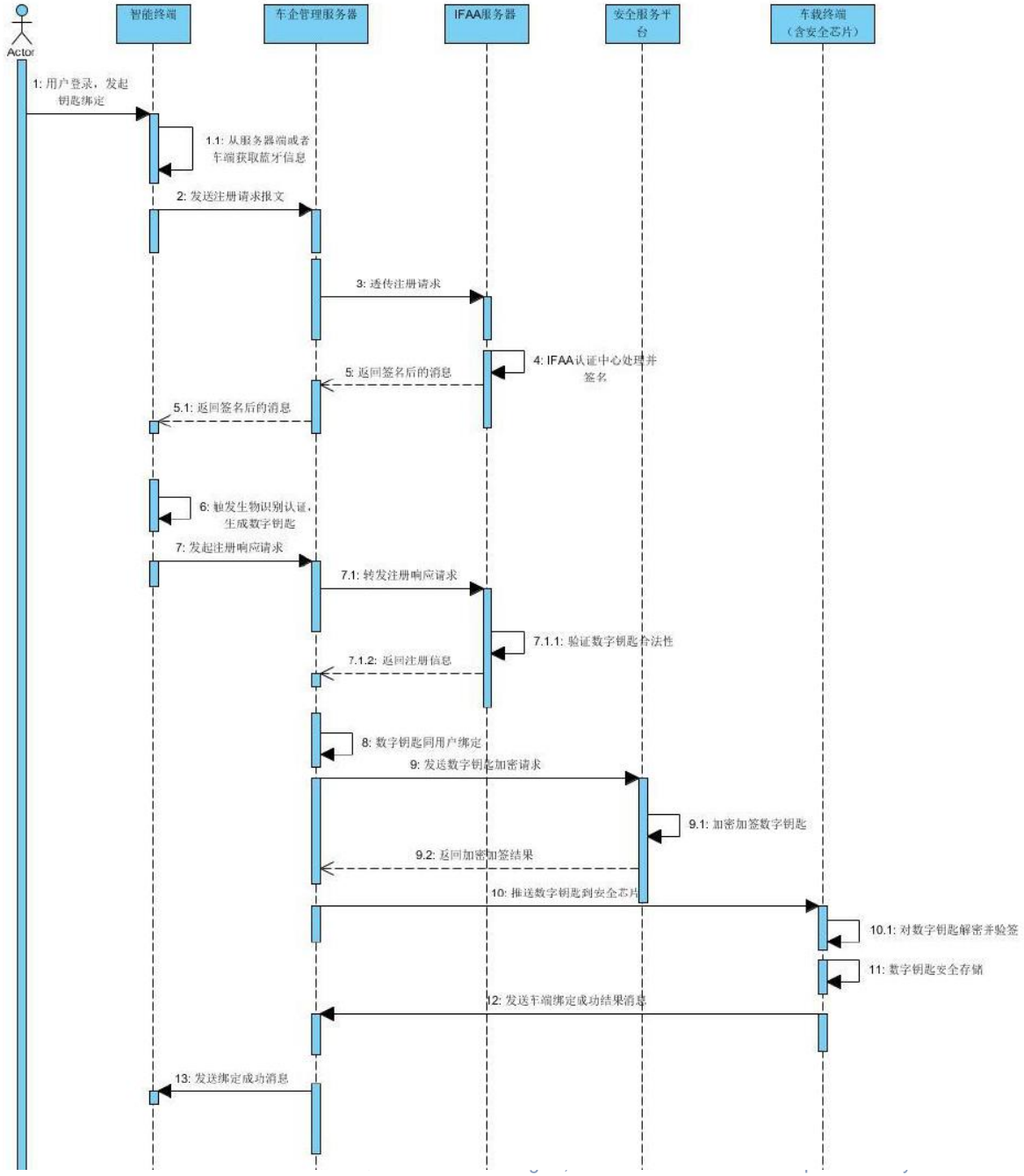
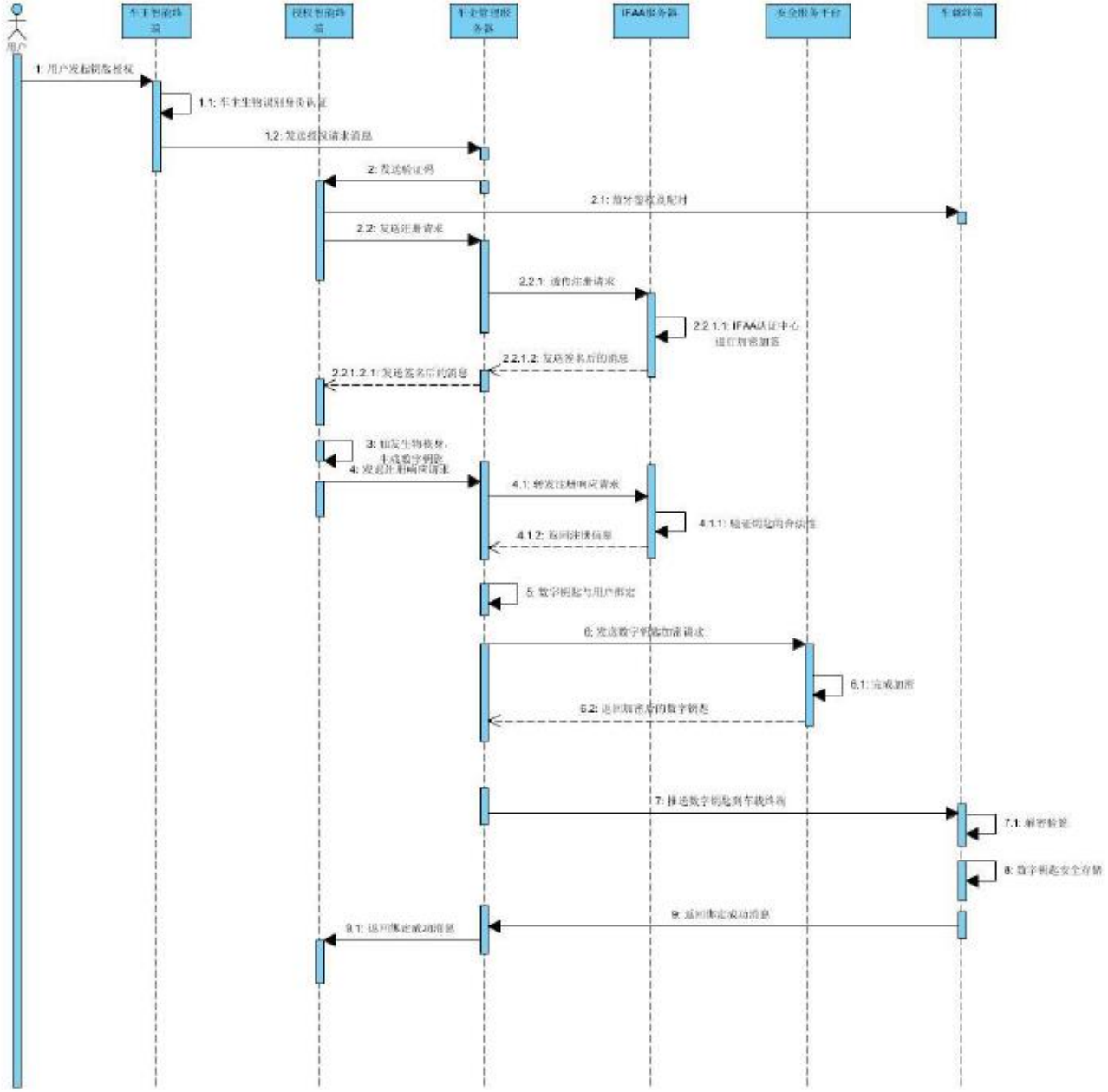


Figure 4-4: OP200b – *DeployService* implementation - AM mode

生成key（IIFAA例）



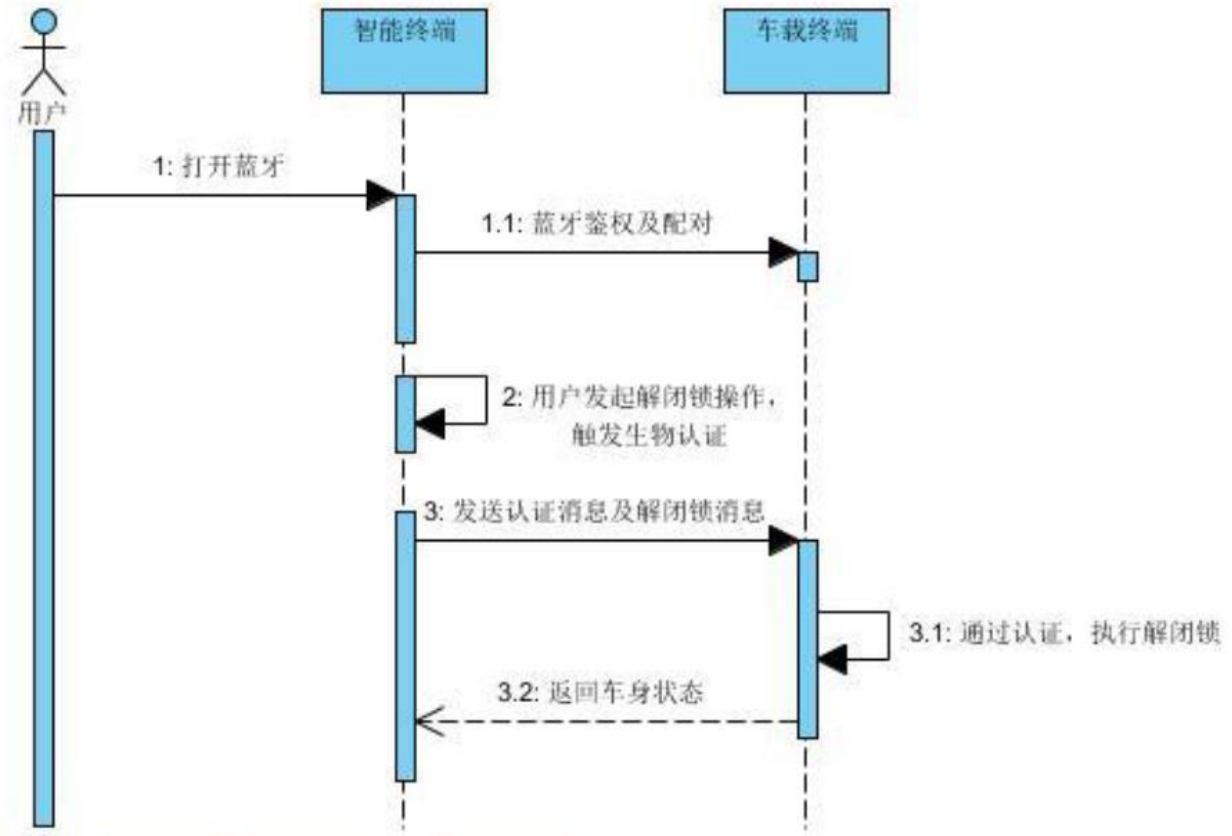
共享key（IIFAA例）



图A.7　厂商数字车钥匙 APP 授权流程（短信验证码方式）

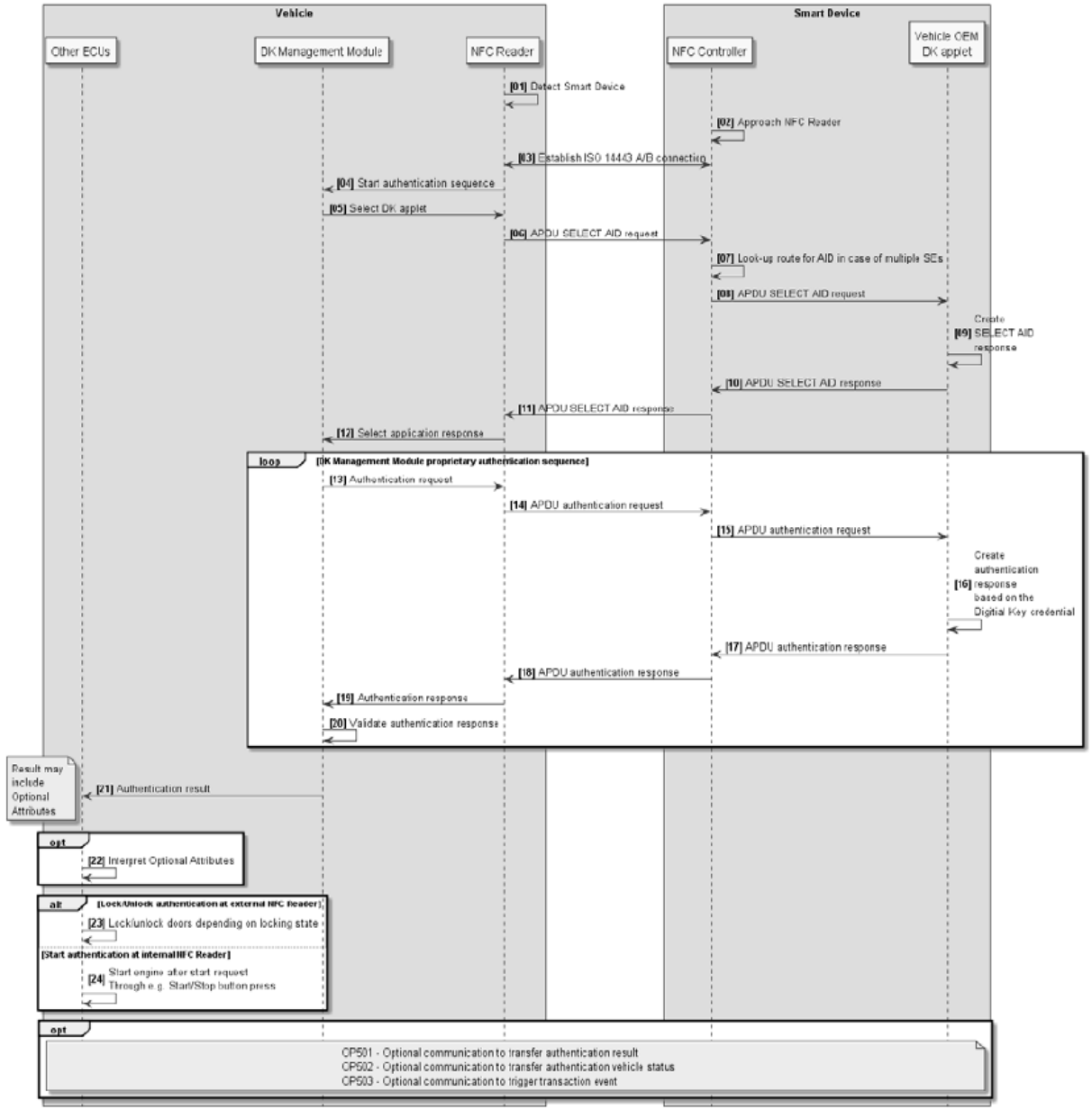
操作（IIFAA例）

T/IFAA 2001-



图A. 5　解闭锁流程

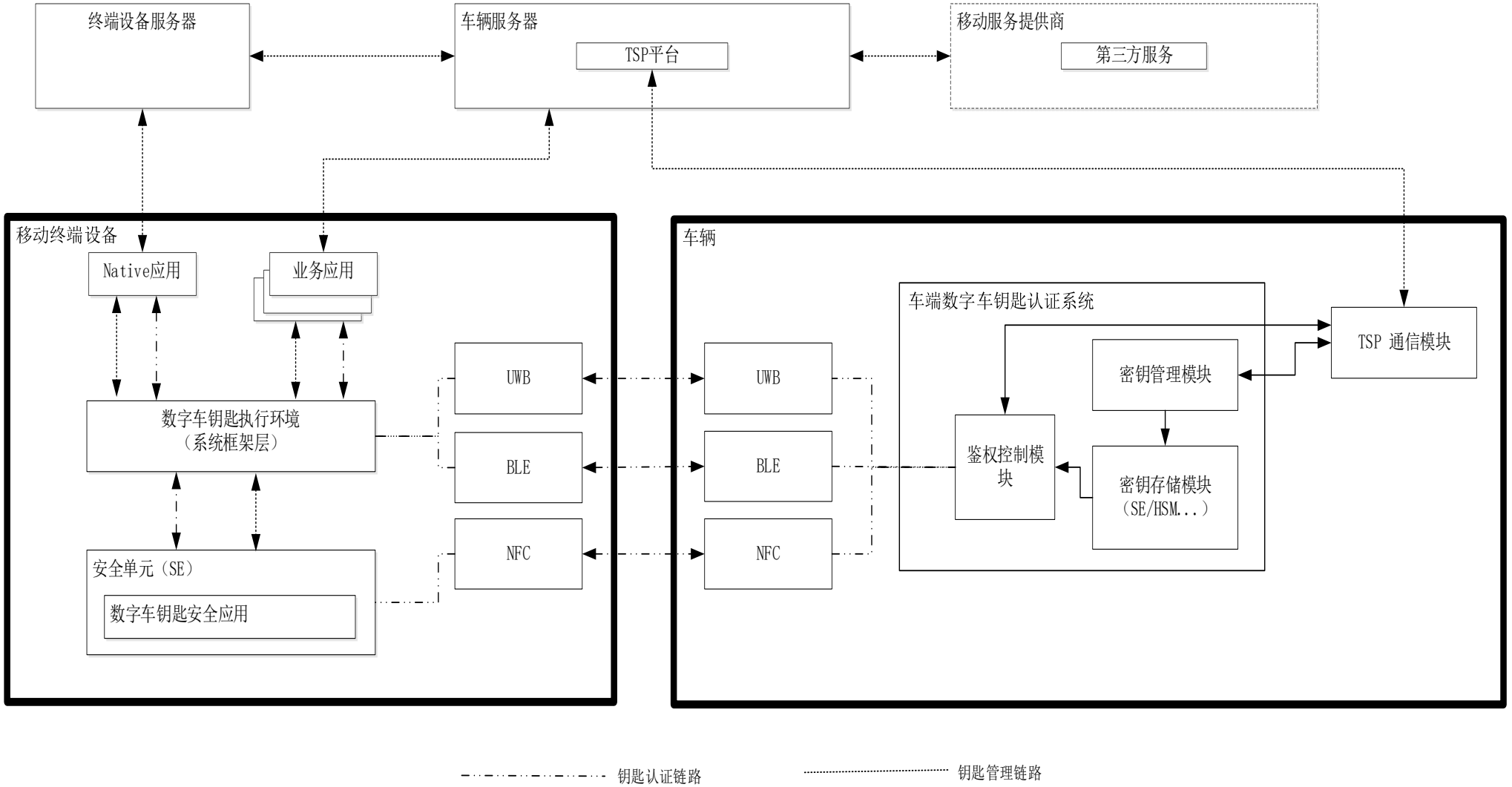
操作（CCCv1.0例）


Vehicle
Smart Device
Other ECUs
DK Management Module
NFC Reader
NFC Controller
Vehicle OEM DK applet
[01] Detect Smart Device
[02] Approach NFC Reader
[03] Establish ISO 14443 A/B connection
[04] Start authentication sequence
[05] Select DK applet
[06] APDU SELECT AID request
[07] Look-up route for AID in case of multiple SEs
[08] APDU SELECT AID request
Create
[09] SELECT AID response
[10] APDU SELECT AID response
[11] APDU SELECT AID response
[12] Select application response
loop
[DK Management Module proprietary authentication sequence]
[13] Authentication request
[14] APDU authentication request
[15] APDU authentication request
Create authentication
[16] response based on the Digital Key credential
[17] APDU authentication response
[18] APDU authentication response
[19] Authentication response
[20] Validate authentication response
Result may include Optional Attributes
[21] Authentication result
opt
[22] Interpret Optional Attributes
alt
[Lock/Unlock authentication at external NFC Reader]
[23] Lock/unlock doors depending on locking state
[Start authentication at internal NFC Reader]
[24] Start engine after start request Through e.g. Start/Stop button press
opt
CP501 - Optional communication to transfer authentication result
CP502 - Optional communication to transfer authentication vehicle status
CP503 - Optional communication to trigger transaction event

IIFAA和CCC对比

- 协议描述角度
  - IIFAA将手机视为一体，描述网元间行为 （IIFAA的流程描述在资料性附录）
  - CCC侧重于将利益相关方间的行为，描述利益相关方的在不同实体上的操作以及配合；尤其是区分“私有接口”
  - CCC描述服务部署管理过程，IIFAA未描述
- 安全要求差异
  - CCC要求SE，IIFAA基本要求TEE，增强要求SE
  - IIFAA单独章节描述安全要求，安全要求到终端、服务器、存储、通信等
- 体系结构差异
  - IIFAA中心化，依赖于IIFAA认证中心
  - CCC以车企为中心，终端企业支持CCC的提供接口，与车企间自动化接口

CCSA数字车钥匙系统架构



CCSA数字车钥匙总体技术要求

- 协议描述角度
  - IIFAA将手机视为一体，描述网元间行为
  - CCC侧重于将利益相关方间的行为，描述利益相关方的在不同实体上的操作以及配合；尤其是区分“私有接口”
  - CCC描述服务部署管理过程，IIFAA未描述
- 安全要求差异
  - CCC要求SE，IIFAA基本要求TEE，增强要求SE
  - IIFAA单独章节描述安全要求，安全要求到终端、服务器、存储、通信等
- 体系结构差异
  - IIFAA中心化，依赖于IIFAA认证中心
  - CCC以车企为中心，终端企业支持CCC的提供接口，与车企间自动化接口

CCSA/TAF数字车钥匙安全要求

- 架构同技术要求
- 分实现场景描述安全要求，包括软件实现，TEE实现，SE实现等
- 分安全能力级别1~3（基本上按软硬件能力）

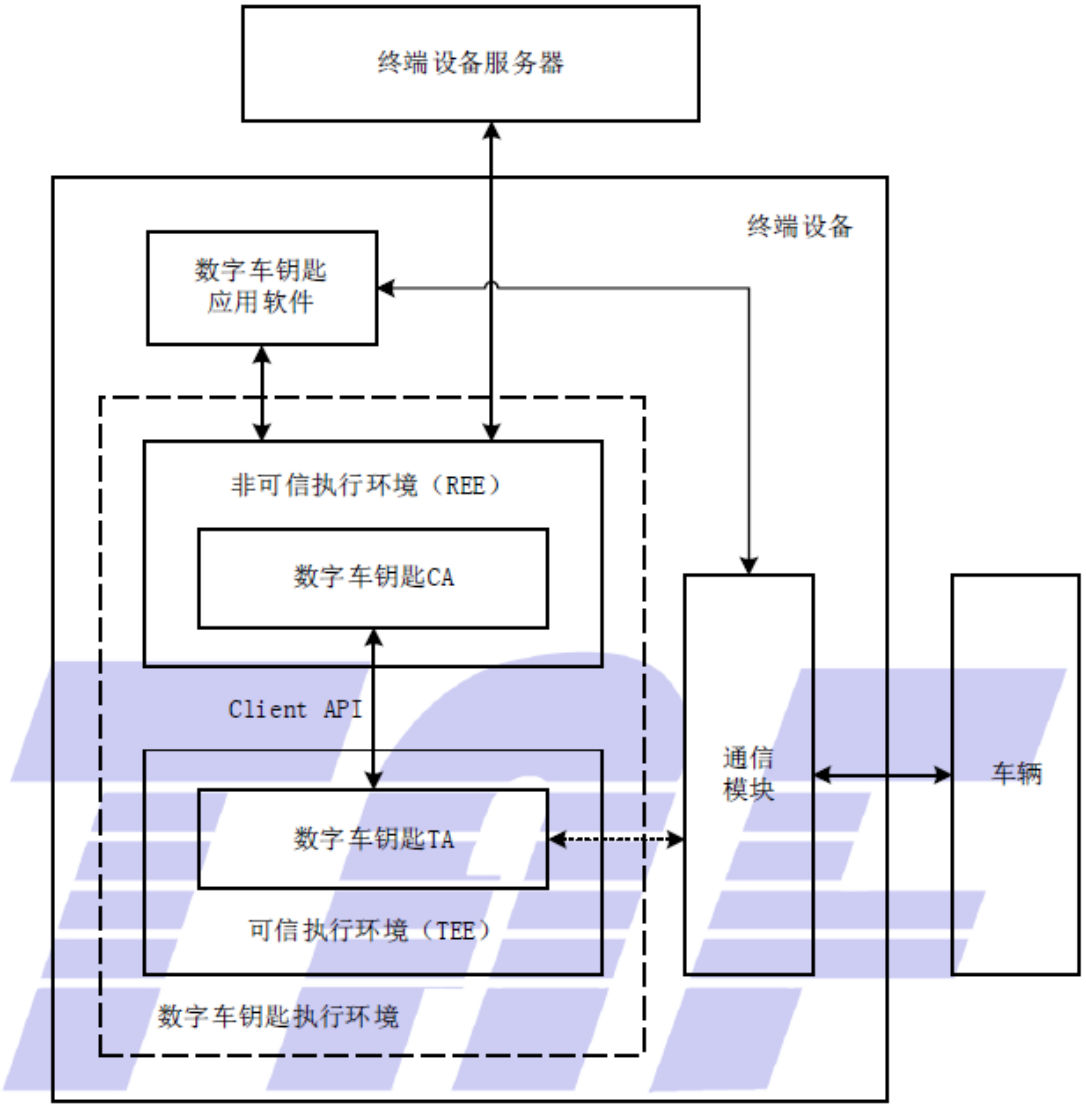


图3　数字车钥匙执行环境 TEE 实现架构图

总结

组织	标准	内容	状态
CCC	CCC-TS-092 **Car Connectivity Consortium Digital Key Technical Specification**	功能，流程，格式，要求，生态角度描述 V2.0 NFC，v3.0 BLE+UWB	V2.0
IIFAA	IIFAA数字车钥匙系统技术规范	功能，流程，格式，要求，网元角度描述 蓝牙	v1
CCSA	基于移动互联网的虚拟车钥匙信息安全技术要求 基于移动互联网的数字车钥匙通信技术要求 基于移动互联网的数字车钥匙总体技术要求	系统架构，各部分功能，连接关系，技术要求 流程，通信协议 安全要求	ongoing
TAF	074移动智能终端数字车钥匙信息安全技术要求	安全技术要求	v1
ICCE	数字车钥匙系统 第 1 部分：总体要求 数字车钥匙系统 第 2 部分：蓝牙系统规范	公开信息： 架构， 蓝牙	v1

读后感

- 生态模式
- 服务架构
- 标准化哪些内容
- 技术方案选择（例如对称vs非对称，生成分发模式等）
- 适用范围和安全性要求的矛盾
- 可扩展性

Qualcomm

Thank you

Follow us on:

For more information, visit us at:

www.qualcomm.com & www.qualcomm.com/blog