

数字钥匙服务稳定性方案及应用

张艳明 刘宇 韩微微 黄殿辉

北京汽车研究总院有限公司 北京 100176

【摘要】：数字钥匙作为智能网联汽车的一部分，核心在于将传统物理钥匙的功能数字化，通过加密通信技术与智能终端结合，实现安全、便捷的权限控制体系，一般由手机端、车端、云端组成。考虑到数字钥匙的安全设计复杂度，主机厂会采用技术外委的方式进行数字钥匙功能的开发；同时为了规避单一供应商带来的管理风险，会选购行业内不同的数字钥匙供应商产品进行车型适配接入。在此背景下，数字钥匙在实际运营、运维过程中会出现主机厂依赖数字钥匙供应商的运维服务排查问题、服务出现异常后响应不及时等问题。本文将围绕主机厂自主提升数字钥匙服务稳定性为出发点，进行问题分析和改进建议。

【关键词】：数字钥匙；管理；服务稳定性

DOI:10.12417/2705-0998.25.15.021

绪论

主机厂通过技术外委的方式完成数字钥匙核心功能开发是普遍现象，比如数字钥匙供应商银基，在过去几年时间里已经覆盖包括特斯拉等超过 12 家主流主机厂和造车新势力^[1]。说明数字钥匙本身有技术壁垒，容易让主机厂在数字钥匙技术中对供应商产生依赖。

数字钥匙将传统车钥匙的全部功能映射到手机中，通过操作手机钥匙实现开关车门、启停发动启后后备箱等功能^[2]。从用户的角度出发，手机数字钥匙取代传统的汽车钥匙无疑带来便利性。但当数字钥匙的服务端出现异常、波动后，会导致服务异常时间段内的申请、分享、注销钥匙失效，进而导致相关控车功能完全失效，引发市场批量问题和用户抱怨。

数字钥匙功能的实现一般涉及主机厂的多方系统协作、部门参与，如 PKI 系统、工厂 MES 系统。此外，主机厂在不同车型上会有选择性的配置蓝牙钥匙、NFC 卡片钥匙、NFC 手环钥匙等数字钥匙功能。跨部门协作、多功能支持，无疑对数字钥匙服务的稳定性会有更高的要求。

基于数字钥匙多供应商支持、多系统对接、多功能选配的特点，文章以云端数字钥匙服务的视角阐述主机厂如何提升服务稳定性。

1 数字钥匙的产品特点

数字钥匙一般由手机端、车端、云端组成，通常主机厂选择同一家供应商进行技术外委，如图 1 所示，外委内容包括数字钥匙手机蓝牙 SDK、数字钥匙服务、车端 PKC，即数字钥匙供应商深度参与了整体的功能设计。同时，如果主机厂在蓝牙钥匙的基础上还要搭载 NFC 卡片钥匙，需要工厂部署写卡客户端向云端数字钥匙服务发送请求进行写卡、激活，这就涉及到了跨公司主体的系统服务调用。

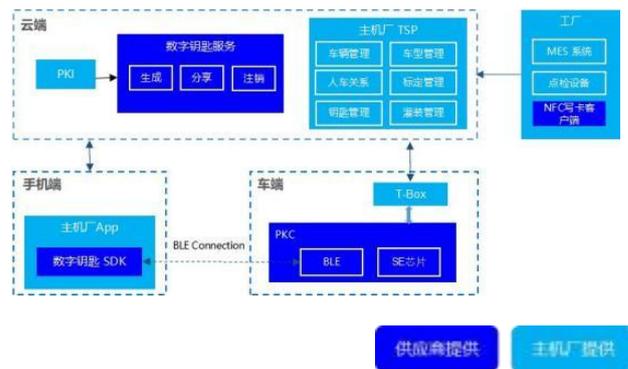


图 1 数字钥匙系统架构

2 数字钥匙服务的常见问题

2.1 数字钥匙服务异常波及范围广

如图 1 所示，APP 端和写卡客户端的申请、分享、注销业务都是由云端数字钥匙服务处理。而 APP 端会将数字钥匙功能与车辆启动功能进行绑定^[3]。一旦数字钥匙服务出现异常、宕机等问题，除了影响市场用户端，还会影响工厂产线正常的车辆配卡、车辆下线，进而引发用户索赔、产线车辆积压等问题。

2.2 数字钥匙供应商管控问题

数字钥匙供应商一般会提供完整的服务和方案直接部署到主机厂。如果主机厂接入多个数字钥匙供应商，不进行业务整合，需要运营人员、技术支持人员了解不同的系统操作习惯，直接增加运营管理成本。

数字钥匙供应商是整体方案的设计者，本身不直接运营数字钥匙功能，更擅长于识别问题、协助分析问题。而对数字钥匙的服务稳定性设计和服务部署架设计，更多的是停留在理论上或借鉴协助已有量产项目分析问题的经验。

数字钥匙供应商因为提供的是整套解决方案，所以配备的运维人员少，且运维人员没有主机厂专业度高。

在量产后，数字钥匙供应商也只是更多的参与问题排查，而非功能使用，也无法直接对话用户了解使用体验。

3 数字钥匙服务设计要点

从主机厂更多的能深度参与数字钥匙运维管理、掌握核心技术的角度出发，主机厂应该在设计阶段就进行深度的参与。

3.1 平台化建设减少管理冗余

如图 1 所示，数字钥匙云端会包括主机厂 TSP 平台，但是数字钥匙的业务相对独立，可作为平台单独管理^[3]。在数字钥匙供应商提供完成的管理平台前提下，主机厂应该识别平台功能项，确认差异功能，将已有的功能进行适配接入，差异功能明确使用场景后与已有的数字钥匙平台进行整体整合。平台化建设一是便于运营人员操作系统，减少错误操作；二是便于发生问题后快速分析解决问题。

3.2 完善数据传输过程中的校验机制

如图 1 所示，实际参与数字钥匙业务的系统很多，至少包括工厂 MES、主机厂 TSP、PKI、手机 SDK、TBOX、PKC。以钥匙生成为例，需要用到由工厂电检从车端获取的车辆信息（VIN、SEID）。为了保证数据完整、有效的存储到云端，避免数字钥匙生成失败，应在数据传输的各环节都进行数据校验，例如：

TSP 收到工厂车辆数据时，判断 SEID 等车辆关键参数是否为空，是否重复，并将错误结果返回工厂；

TSP 收到车辆信息后，以推送机制同步至数字钥匙服务，避免 TSP 服务异常时查询不到数据；

TSP 在推送的基础上增加查询接口，在数字钥匙服务获取不到车辆数据时主动向 TSP 查询，避免因推送异常造成的查询不到数据。

3.3 工具化管理追溯记录

数字钥匙的数据管理应该更多的使用工具。除了主机厂内部会有云端数字钥匙管理平台管理钥匙生命周期与 MES 工厂做系统对接以外^[4]，还有数字钥匙 SE 芯片供应商的灌装数据的外部系统对接。但 SE 芯片供应商工厂端普遍没有系统对接的能力，所以一般由主机厂负责芯片的工程师以邮件往来的方式向芯片厂商下订单用于确认芯片灌装数据。邮件传递的方式本身存在安全风险，且不方便工程师追溯订单记录。可以使用对象存储（比如阿里云 OSS），主机厂通过管理平台以类似网盘下载文件的方式进行灌装数据传递。

3.4 制定明确的目标要求

数字钥匙供应商一般会提供技术方案、测试方案、部署方案等进行方案评审，主机厂应对核心内容制定明确的目标。比如在数字钥匙服务的性能压测期间，应严格关注、约束核心性能指标结果，减少量产用户对用户的使用体验上的影响，提出性能要求包括：性能评价 Apdex 范围（满意度）大于 0.85；90% 的业务请求响应时间控制在 1-2 秒。在性能压测期间，如果暴

露出负载不均、数字钥匙功能不能使用等异常情况，应及时与供应商沟通，以调整程序、调整服务配置、增加服务资源、复测复现等方案进行问题处理解决。

4 数字钥匙服务线上告警监控

当数字钥匙在 APP 端正式发布在市场上运行时，对于数字钥匙服务的异常问题排查，不能单纯的依赖售后服务人员的客诉反馈。从客诉到问题解决需要经过层层流转，严重影响问题解决效率。主机厂应该具备数字钥匙服务异常监控和服务预警的能力。

4.1 心跳监控告警

通过定期发起 HTTP 请求来监测服务的运行状态，如果服务因故障或其他问题而无法响应，利用飞书或别的方式进行告警通知运维或开发处理。具体可包括：

- (1) 利用阿里云服务的工具配置服务健康检查，接口异常会重启服务；
- (2) 用专业监控工具（比如 zabbix）进度接口异常报警；
- (3) 在服务内部编写程序发起 HTTP 请求，接口异常时报警，开发编写程序。

4.2 日志监控告警

基于阿里云的日志服务(SLS)，可以通过设置关键字告警来监控日志中的特定事件或错误。例如，监控“ERROR”关键字，如果在设定的时间范围内，“ERROR”关键字出现了设定的数量，将触发告警，通过飞书或别的方式发送告警信息。

4.3 告警阈值监控

运维人员设定数字服务的告警阈值监控，超过规定阈值后触发飞书报警。以

图 2 为例：

- (1) ACK 容器 1 临时存储剩余 1G；
- (2) 容器内存利用率大于 90%；
- (3) 容器 CPU 使用率大于 50%；
- (4) Pod 在 60 分钟内，重启次数大于 1 次；
- (5) Pod 状态异常（Pod 启动失败）；



图 2 告警阈值设置

4.4 灰度上线

数字钥匙云端服务如果有新需求或 Bug 修复上线需要生产验证但又想尽量减少对生产环境用户的影响，即可以通过用户白名单模式进行功灰度发布。灰度发布方案支持两种模式：以请求头为判断条件进行请求转发灰度 Pod；或者以请求量百

分比进行请求转发灰度 Pod。这样在灰度发布环境下的用户进行生产环境验证一段时间后,再进行全平台的服务更新。

5 结论

结合数字钥匙系统多系统对接、多供应商管理、云端服务异常造成影响大等特点,主机厂应加强对数字钥匙服务稳定性的把控。

在设计阶段,结合主机厂的实际服务架构、业务实现情况,进行服务的适配兼容符合主机厂管理系统服务的基本流程。并

在设计阶段对测试方案、部署方案进行严格的指标制定。

在测试阶段,关注测试过程中出现的服务异常造成的数字钥匙服务不可用问题。因为此类问题到了正式发布会同样触发变成市场问题、质量问题。

在运维阶段,主机厂起着问题排查的主导作用,联合数字钥匙设计者对服务问题进行根因分析、排查,并针对性的进行服务优化、程序优化。问题排查过程也有助于主机厂深度了解系统涉及逻辑及缺陷,进而逐渐提升产品管控专业能力。

参考文献:

- [1] 单宏寅.数字钥匙当然不只是个 APP.<https://view.inews.qq.com/a/20220620A062RA00>.2022.
- [2] 信瑛南,刘静,李琦,张瀛,董嵩松,丁靖.手机数字钥匙远程控制车辆系统的设计[J].汽车工程师.2018(10).
- [3] 中国汽车技术研究中心有限公司.GB/T XXXXX--XXXX.《汽车数字钥匙系统技术规范》.
- [4] 钟晓敏,苏国传,程登,等.基于汽车数字钥匙系统架构设计与实现[J].现代工业经济和信息化.213:(3)2022.
- [5] 邹涵.基于 Spring Cloud 的灰度发布系统的设计与实现.南昌大学.2024.