ICS 43.040
T 35

团 体 标 准

T/JSSAE 009—2025

汽车数据共享服务安全要求与测试方法

Security requirements and testing methods for automotive data sharing services

2025-11-19 发布 2025-11-30 实施

江苏省汽车工程学会 发 布

目　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由江苏省汽车工程学会提出。

本文件起草单位：中汽院(江苏)汽车工程研究院有限公司、中国汽车工程研究院股份有限公司、重庆长安汽车股份有限公司、赛力斯集团股份有限公司、江苏大学、中检集团天帷网络安全技术（合肥）有限公司。

本文件主要起草人：全代勇、刘冲、雷剑梅、罗薇、雷相其、谢天瀛、曹国华、牟原野、汪向阳、龚静、田甜、陈冬梅、郭云川、韩牟、王芳、严瑞、孙岩炜、贾晓俊、周小贺、韩松、余处和、王维。

本文件为首次发布。

汽车数据共享服务安全要求与测试方法

1 范围

本文件规定了汽车数据共享服务平台和汽车数据共享过程中的安全要求与测试方法。

本文件适用于汽车生产企业、汽车重要零部件供应商和出行服务平台型企业安全合规开展汽车数据共享服务。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069—2022 信息安全技术 术语

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 41871—2022 信息安全技术 汽车数据处理安全要求

T/CCSA 441—2023 车联网服务平台网络安全防护要求

3 术语和定义

GB/T 25069—2022、GB/T 35273—2020和GB/T 41871—2022界定的以及下列术语和定义适用于本文件。

3.1

汽车数据 vehicle data

汽车设计、生产、销售、使用、运维等过程中涉及的车辆数据、个人信息、道路环境数据等数据。

3.2

汽车数据共享服务平台 service platform of vehicle data sharing

为实现汽车数据价值释放为目标的可信共享服务基础设施。

3.3

数据共享应用 vehicle data sharing application

为实现汽车数据价值利用为目标的软件服务系统。

3.4

汽车数据共享过程 vehicle data sharing process

通过技术手段和协议，将汽车数据在合法合规的前提下，从数据源传输至目标方的系统化流程。

4 缩略语

下列缩略语适用于本文件。

TLS：安全传输层协议（Transport Layer Security）

5 概述

汽车数据共享如图1所示，包括数据提供方、数据使用方、共享服务平台三部分。

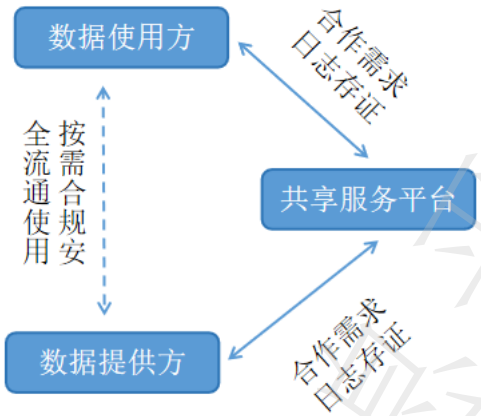

图1　数据共享架构图

6　共享服务平台安全要求

6.1　通用要求

共享服务平台应满足T/CCSA　441—2023中的第三级安全防护相关要求。

6.2　服务主体身份认证

服务主体身份认证要求如下：

a）　主体合法性要求：具备独立法人资格及相应服务资质；
b）　个人身份真实性要求：需提供居民身份证（含临时身份证）、户口簿、护照等法定证件；
c）　单位真实性要求：需提供营业执照、组织机构代码证等，并附加法定代表人授权书。

6.3　访问控制

访问控制要求如下：

a）　应对共享服务平台中的共享数据设置访问控制机制，防止对共享数据的非授权访问；
b）　应对共享服务平台中的共享数据的操作设置权限管理，防止对共享数据的非授权操作；
c）　应对共享服务平台特权账号和特权会话进行安全管控。

6.4　安全审计

安全审计要求如下：

a）　应对共享服务平台中共享数据的各种操作进行审计，如共享数据的上传、修改、下载、复制、删除等；
b）　应对共享服务平台中的连接和传输过程进行审计，如审计共享服务平台与共享应用的连接是否通过认证；
c）　应对共享过程中发生的错误、故障、报警、失败、安全事件日志进行审计；
d）　应对共享数据的内容安全和合规性进行审计，如数据脱敏操作是否完整执行。

7 共享过程安全要求

7.1 通信安全

数据共享服务平台与数据共享应用在通信过程中，应采用TLS1.2版本及以上或至少同等安全级别的安全通信协议建立安全的通信连接，确保数据服务平台与数据共享应用之间通信数据的机密性、完整性等。

7.2 数据安全

数据安全要求如下：

a） 应保证共享数据在传输过程中的机密性和完整性；

b） 应保证共享数据在共享过程中的可鉴别性。

8 测试方法

8.1 服务平台安全测试方法

8.1.1 通用要求测试

检查确认满足T/CCSA 441—2023中的第三级安全防护相关要求。

8.1.2 身份认证测试

身份认证测试方法如下：

a)检查数据共享服务发起共享请求时，服务平台是否对共享应用的真实性进行验证，测试结果应符合服务主体身份认证要求。

8.1.3 访问控制测试

访问控制测试方法如下：

a） 检查服务平台中是否对共享数据设置访问控制机制，测试设置的访问控制机制不能对共享数据进行非授权访问；

b） 检查服务平台中是否对共享数据的操作设置权限管理，逐条测试设置的权限管理策略，不能对共享数据进行非授权操作 ；

c） 检查服务平台中是否对存在特权账号和特权会话进行了安全管控，安全管控措施包括技术手段和管理手段。

8.1.4 安全审计测试

安全审计测试方法如下：

a） 对服务平台中的共享数据进行下载、修改和删除操作，检查平台是否记录了相应操作的日志；

b） 使用测试工具模拟进行数据共享，检查是否记录了建立连接的过程和数据传输的日志，测试共享服务平台与共享应用的连接是否通过认证；

c） 使用测试工具对共享过程中发生的错误、故障、报警、失败、安全事件日志进行审计，实现对平台 6 个月内异常行为可追溯；

d） 使用测试工具进行合规性验证，并定期开展合规审计。

8.2 共享过程安全测试

8.2.1 通信协议测试

通过抓包分析通信数据，检查通信双方是否使用TLS1.2版本以上或至少同等安全级别的安全加密协议（如TLCP等），并检查双方通信数据的机密性、完整性等是否得到保护，测试结果应符合7.1的要求。

8.2.2 数据安全测试

a） 检查服务平台是否将共享数据密钥存储在专用安全可信的存储空间，尝试设置代理并使用数据抓包工具进行抓包；

b） 使用测试工具模拟进行数据共享,检查是否采用数字签名等技术措施。

参 考 文 献

［1］ 国家信息中心信息《国家信息中心：数据共享安全框架研究》