ICS 35.040
CCS L 79

SJ

中华人民共和国电子行业标准

SJ/T XXXXX—XXXX

车联网数据共享安全架构

Data sharing architecture of internet of vehicles

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国工业和信息化部　　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。

本文件由中华人民共和国工业和信息化部提出。

本文件由中国电子技术标准化研究院归口。

本文件起草单位：电子科技大学、中国电子技术标准化研究院等。

本文件主要起草人：

车联网数据共享安全架构

1 范围

本文件规定了车联网数据的安全共享架构，并规定了该架构下车联网数据的安全共享过程及各业务环节的安全要求。

本文件适用于支持车联网数据进行安全共享的系统、平台的设计开发、应用部署和维护管理。

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 22239—2019 信息安全技术 网络安全等级保护基本要求
GB/T 25069—2022 信息安全技术 术语
GB/Z 28828—2012 信息安全技术 公共及商用服务信息系统个人 信息保护指南
GB/T 35273—2020 信息安全技术 个人信息安全规范
GB/T 36073—2018 数据管理能力成熟度评估模型
GB/T 37935—2019 信息安全技术 可信计算规范 可信软件基
GB/T 39412—2020 信息安全技术 代码安全审计规范
GB/T AAAAA 智能网联汽车数据通用要求

3 术语和定义

GB/T 25069—2022界定的以及下列术语和定义适用于本文件。

3.1

车联网数据 data of internet of vehicles

由车辆、道路交通监测和控制设备、驾乘人员等产生的，通过车联网传输的数据。

注：一般包括车辆的基础数据、工况数据、环境感知数据、通信数据、应用服务数据，道路交通的地图数据、路侧感知数据、交通控制和引导数据，驾乘人员的基础数据、出行数据、行为数据、应用服务数据等。

3.2

数据目录 data directory

展示车联网数据的内容描述、数据类型、数据量、数据摘要等数据描述信息的目录。

3.3

数据应用 data application

对数据进行处理、分析、计算以得到所需结果的应用程序。

3.4

数据节点 data node

用于存储数据和执行数据相关操作的实体。

3.5

数据提供方 data-providing party

产生和/或采集车联网数据并共享数据的相关主体。

注：一般为汽车厂商、道路交通管理部门以及其他车联网信息服务提供商等。

3.6

数据使用方 data-utilizing party

使用车联网数据并基于数据提供服务的各类相关主体。

注：一般为汽车厂商、车联网信息服务提供商、道路交通管理部门、个人和企业用户等。

4 缩略语

CA：认证机构(Certificate Authority)

SSL：安全套接层(Secure Sockets Layer)

TLS：传输层安全（Transport Layer Security）

VIN：车辆识别号码(Vehicle Identification Number)

5 通则

5.1 安全共享架构

车联网数据一般以分布式的方式存储在数据提供方管理的数据节点中。为了保障数据的安全，数据使用方不应直接访问数据节点中的车联网数据，而应以“对方计算”的方式使用车联网数据。即数据使用方将数据应用代码传输到数据提供方的数据节点中，在数据节点进行车联网数据的处理和计算，最终获取数据应用产生的计算结果；而数据提供方提供数据目录和数据应用代码的运行环境，以此方式保障车联网数据的安全。为了实现车联网数据的广泛共享，一般通过车联网数据共享平台对多个数据提供方的数据资源进行整合，同时对数据使用方和其数据应用进行鉴权和访问管理，并监测两者间传输的数据。

车联网数据的安全共享架构如图1所示。

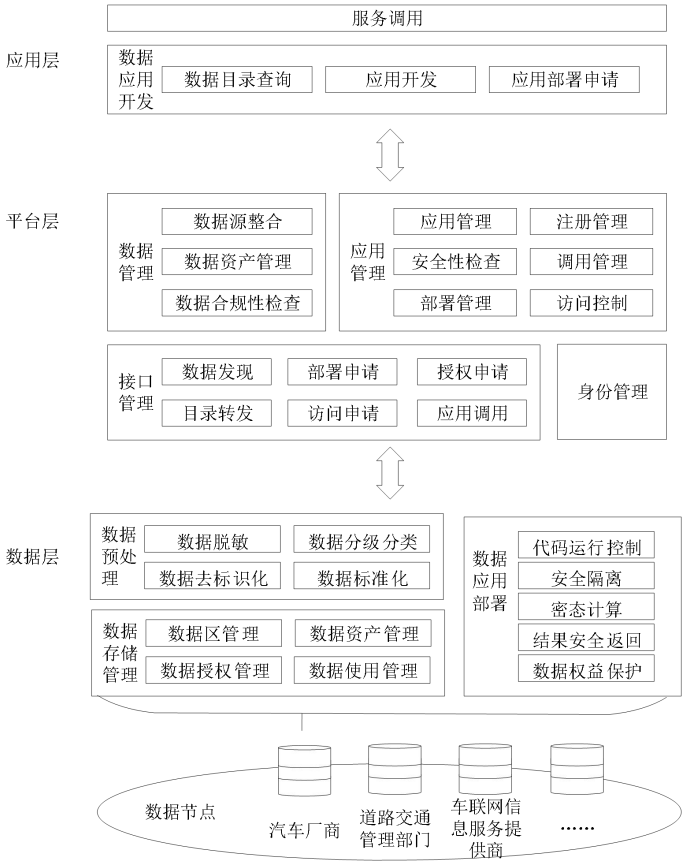

图 1 车联网数据的安全共享架构

车联网数据的安全共享架构包含三个层级：

——数据层，包含多个数据提供方的数据节点，每个数据节点都储存和管理车联网数据，并提供数据应用运行环境。数据层并不对外传输车联网数据本身，而是传输数据目录和数据结构概要信息；

注：数据结构概要信息包括元数据和示例数据。

——平台层，提供数据安全交互的基本架构和安全技术体系，以确保数据共享全流程安全合规。负责将数据层的数据目录和数据结构概要信息转发应用层，同时将应用层的相关请求转发数据层相应的数据节点，并返回请求结果。数据层和应用层的所有交互，均需要通过平台层的安全管理；

——应用层，包括数据应用开发和各种应用服务。应用层不直接请求和获取车联网数据，而是将开发的数据应用通过平台层传输和部署至数据层相应的数据节点，获取数据应用计算后的结果并在相关应用服务中使用。

5.2 安全共享过程

车联网数据的安全共享过程如图2所示。

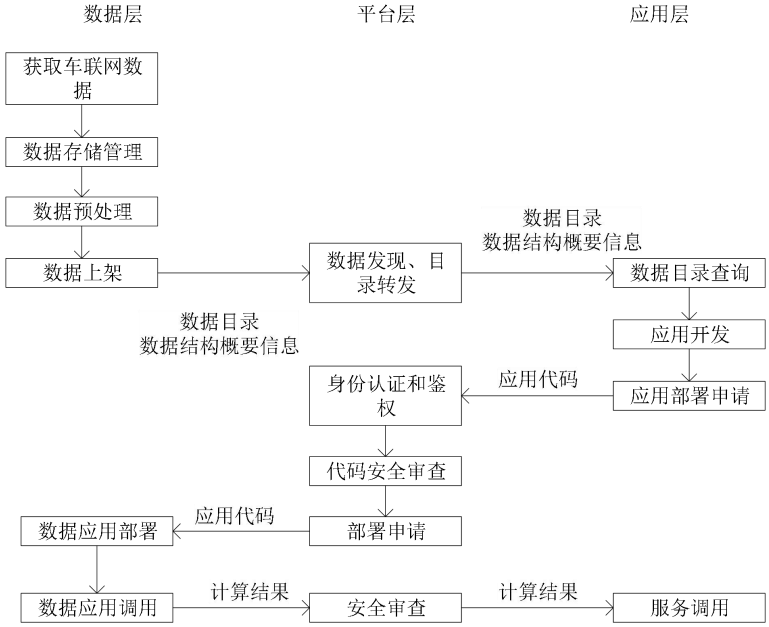

图 2 车联网数据的安全共享过程

安全共享过程主要包括：

a) 数据提供方获取和储存车联网数据，在数据层对原始车联网数据进行预处理后完成数据上架；
b) 数据上架后，平台层公布和转发数据目录和数据结构概要信息；
c) 数据使用方根据业务需求，基于了解的数据目录和数据结构概要信息进行数据应用的开发；
d) 数据使用方向提交数据应用代码并申请部署；
e) 平台层对数据使用方进行鉴权和身份认证，并对数据应用代码进行安全审查，通过后申请再数据节点部署数据应用；
f) 数据层在数据应用运行环境中部署数据应用，调用后产生所需的计算结果；
g) 计算结果通过平台层返回给应用层，数据使用方根据这些计算结果进一步提供车联网信息服务。

在车联网数据共享过程中的安全要求见第6章。

6 安全要求

6.1 通用要求

6.1.1 安全基础措施

车联网数据共享过宜符合GB/T 36073—2018中数据集成与共享程度的优化级要求。

车联网数据共享过程中，应建立数据安全机制，提供安全可靠的数据交换方案，保障数据全生存周期的安全可控。

应按照GB/T 22239—2019中第8章的第三级安全通用要求建立数据基础安全措施。

6.1.2 密码算法

应使用符合相关国家或行业标准的密码算法或密码技术，包括但不限于对称密码技术、非对称密码技术、标识密码算法等，保以障数据的保密性、完整性和不可抵赖性。

应符合GB/T 39786中对密钥管理的要求，对密钥的生成、存储、分发、使用、备份、恢复、销毁等环节进行管理。

6.1.3 数据传输

在传输数据时应使用SSL/TLS密码协议来保障数据传输过程中的完整性、机密性和不可抵赖性。数据节点应：

a) 具备监控数据传输过程的能力，发现安全问题时及时告警并断开传输。
b) 具备在数据传输不完整时清除传输缓存数据的能力。
c) 数据传输完成后清除历史缓存数据。
d) 定期检查或评估数据传输的安全性和可靠性。

6.2 数据存储管理

数据提供方产生和获得的车联网数据存储在数据节点，并：

a) 应通过冗余技术对数据节点存储的车联网数据进行保护，防止突发情况下数据的丢失；
b) 应按照数据分级分类相关要求，对安全等级达到三级以上的敏感数据进行加密存储。
c) 宜采用去中心化、点对点等的数据节点部署模式，提高车联网数据的安全共享架构的公信力；
d) 应在物理上确保数据节点受控；
e) 应在数据节点处使用 CA 认证以保障合法注册；
f) 应支持数据逻辑存储，以满足不同数据类型、不同数据容量和不同数据用户的逻辑存储管理；
g) 宜建立分层的逻辑存储授权管理和授权操作规则，实现对数据逻辑存储结构的分层和分级保护；
h) 应对访问车联网数据的用户进行身份鉴别和权限控制，并对用户权限变更做相应的审核并保留记录以满足审计要求；
i) 应为数据节点管理员提供用户标识与鉴别策略、数据访问控制策略，包括访问控制时效的管理和验证、接入数据存储的合法性和安全性认证等；
j) 应对数据节点中批量修改、拷贝、下载等重要操作权限进行限制。

此外，应提供数据区管理、数据资产管理、数据授权管理、数据使用管理等功能。

6.3 数据预处理

数据层的相关数据节点应对原始车联网数据进行数据预处理，应满足隐私保护的要求，包括：

a) 应采用多种数据脱敏处理方法过滤原始车联网数据中的隐私敏感数据，保证数据的隐私安全，个人敏感数据的判定应按照 GB/T 35273—2020 附录 B 的方法进行，车辆敏感数据的判定应符合 GB/T AAAAA 中的要求；
b) 应对有潜在标识风险的关键数据字段进行匿名化或去标识化处理，以降低数据泄露的风险。例如，车辆信息应按照 GB/T 35273—2020 中 6.2 的要求，对车辆识别号（VIN）进行匿名化或去标识化处理；
c) 应按照 GB/T AAAAA 要求确定车联网数据分级分类规则，对车联网数据进行分级分类存储和管理。

d) 应制定车联网共享数据的标准格式，并以标准格式进行归类存储，提供数据目录和数据结构概要信息。

6.4 数据上架

数据层应向平台层公开可共享的数据目录和数据概要信息，即数据上架。数据上架前应确立数据的权益，明确数据的来源和使用限制，并采用安全可信的技术机制和手段，对数据权属进行登记和审计。

6.5 身份管理

平台层应建立完备的身份管理机制，包括：

a) 宜采用 CA 证书或非对称密码技术的公钥作为用户的身份凭证，该凭证具有唯一性，用户私钥可保存在安全智能卡设备中或加密存放，以避免用户身份被冒用；
b) 应按 GB/T 22239—2019 中 8.1.4.1 提出的要求，提供基于密码学技术的身份认证；
c) 应对访问数据处理系统、服务器操作系统、数据库系统、备份系统的管理员进行身份鉴别，鉴别过程中不应传送身份凭证的私有部分，宜采用数字签名等技术确保安全性；
d) 应建立口令管理策略，包括用户口令长度、口令生存周期、口令复杂度等，保障基于口令的身份鉴别安全性；
e) 对敏感数据或重要模块的操作应采用两种或两种以上的鉴别技术进行身份鉴别；
f) 应设置身份凭证使用期限，过期的身份凭证应重新审核或自动失效。对于已作废的身份凭证，应保留其过去的登陆与操作信息。

6.5.1 访问控制

平台层应建立完备的访问控制机制，包括：

a) 应定期检查数据节点数据交换操作的授权，并按照授权策略执行访问控制，拒绝不符合授权的访问，保留授权检验记录；
b) 宜自动监视和控制远程访问会话，以检测非授权的访问行为；
c) 应根据角色和应用场景建立用户操作行为列表，并设置用户权限。

6.6 安全审计

平台层应建立安全审计机制，以防止可能的误用或未授权的访问。安全审计的要求包括：

a) 应对数据使用及处理全过程进行安全审计；
b) 应对数据库日志、系统日志进行全面审计；
c) 应具备跟踪和记录数据集成、分发等能力，以支持数据溯源；
d) 审计日志应至少保存 6 个月。

6.7 数据应用部署

数据应用部署过程中平台层和数据层应进行代码检查、部署鉴权、安全部署和安全存储：

a) 应保障数据应用的代码安全，应明确数据应用代码安全标准并采用代码扫描或源码审查工具对数据应用程序进行代码安全检查，并按 GB/T 39412—2020 的要求进行代码安全审计；
b) 在部署应用程序时应进行身份鉴别和权限验证，根据其权限，选择合适的部署方案，确保数据应用的功能和性能符合要求；
c) 应在部署数据应用前对部署方案进行验证，确认无误后才可执行部署操作。代码上传过程中应保障代码的完整性和保密性；
a) 在数据节点成功部署的代码应在数据节点的安全存储空间中加密存储，保障数据应用开发方代码不被窃取、不被逆向工程解析。应按 GB/T 37935—2019 中 9.2.3 的要求，对执行环境中的程序代码片段进行完整性保护，防止非法篡改。

6.8 应用调用

应用调用时平台层应进行身份鉴别和权限验证，此外，数据层还应符合运行隔离、代码运行控制、数据权益保护、结果安全返回等安全要求。

a) 宜采用基于软件、硬件或软硬件结合的安全沙箱机制，为应用代码提供安全的隔离计算环境，保证运行过程中代码及数据的安全。

b) 为保证数据应用的正确性和安全性，在应用代码运行中：
   1) 应确保对数据的操作符合授权，不应超出权限范围或违反权限约束；
   2) 不应修改、删除和转移存储在数据节点中的车联网数据；
   3) 应只返回数据的分析结果，不应泄露原始数据的内容或结构；
   4) 应实施有效的访问控制，确保只有授权用户和授权应用能够访问数据。访问控制符合 6.7 的要求。

b) 为保证数据应用的合法性和可追溯性，数据应用的运行应遵循以下规则：
   1) 数据应用的运行应视为对数据资产的使用，应尊重数据权利人的权益，不得侵犯数据的所有权、使用权和收益权；
   2) 应记录数据应用与数据的交互细节并生成操作日志，记录内容包括数据应用的名称、版本、数据来源、数据目的、数据范围、运行时间、交互动作、运行结果、交互数量等；
   3) 操作日志应被可信地记录和存储，不得被篡改或删除，必要时应提供给安全审计机构进行检查和验证。

c) 为保障数据应用的隐私性和效率性，在关联和整合数据应用的结果时应：
   1) 采用数据隐私保护技术，防止数据应用的结果被泄露或篡改；
   2) 结合可信计算环境、多方安全计算、同态加密、零知识证明、群签名、环签名、混淆技术等技术，实现在加密数据上的高效运算；
   3) 根据数据应用的特性和需求，选择合适的数据隐私保护技术，确保数据应用的结果的正确性和可信度。