ICS 07.040
CCS A 75

CH

中 华 人 民 共 和 国 测 绘 行 业 标 准

CH/T XXXXX—XXXX

智能汽车基础地图数据传输安全保护技术规范

Technical specification of transmission security protection for intelligent vehicle basic map data

(点击此处添加与国际标准一致性程度的标识)

（报批稿）

（本草案完成时间：2025 年 1 月 7 日）

－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国自然资源部　　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。

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。

本文件由中华人民共和国自然资源部提出。

本文件由全国地理信息标准化技术委员会测绘分技术委员会（SAC/TC 230/SC2）归口。

本文件起草单位：中国测绘科学研究院、北京华为数字技术有限公司、易图通科技（北京）有限公司、北京百度智图科技有限公司、高德软件有限公司、北京四维图新科技股份有限公司、腾讯大地通途（北京）科技有限公司、自然资源部信息中心、中电科网络安全科技股份有限公司、北京百度网讯科技有限公司、中国信息通信研究院、北京初速度科技有限公司。

本文件主要起草人：马小龙、赵园春、方驰宇、马照亭、费雯凯、汤咏林、李宏利、于迅文、石一慧、邵冬华、朱大伟、王月明、李泽慧、彭建芬、温旭杰、王健、房骥、冯晓林。

智能汽车基础地图数据传输安全保护技术规范

1 范围

本文件规定了智能汽车基础地图数据的传输场景、基本要求、安全保护方法和证实方法。

本文件适用于智能汽车基础地图数据在车载终端、路侧终端与地图专有平台之间传输的安全保护。

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 37092 信息安全技术 密码模块安全要求

GB/T 38636 信息安全技术 传输层密码协议（TLCP）

GB/T 43206 信息安全技术 信息系统密码应用测评要求

GM/T 0008 安全芯片密码检测准则

3 术语和定义

下列术语和定义适用于本文件。

3.1

智能汽车基础地图数据 intelligent vehicle basic map data

支撑智能汽车驾驶自动化系统的导航电子地图产品数据，以及智能汽车传感器产生的具有时间和空间特征的地理信息数据。

注 1：智能汽车指具备环境感知、智能决策、自动控制等功能的汽车。

注 2：智能汽车基础地图数据类型包括产品数据和传感器数据。

注 3：产品数据是用于提供公开地图产品服务的数据；传感器数据是用于产品数据制作、更新和使用等的地理信息数据，包括卫星导航定位接收机、惯性导航装置、摄像头、激光雷达及毫米波雷达等传感器产生的数据。

3.2

地图专有平台 map proprietary platform

提供智能汽车基础地图数据（3.1）接收、处理、更新和服务，存储、计算和网络资源独享，具备弹性按需特性的计算平台。

3.3

路侧终端 road side unit

安装在道路两侧或门架上，利用现代通信技术进行信息发送和接收的功能实体。

[来源：JT/T 1458—2023，定义3.3，有修改]

3.4

车载终端 on board unit

安装在智能汽车上的具备信息采集、处理及利用现代通信技术进行信息发送和接收的功能实体。

[来源：JT/T 1458—2023，定义3.2，有修改]

3.5

地图专有平台证书 map proprietary platform certificate

用于智能汽车基础地图数据（3.1）传输过程中标识地图专有平台身份信息的数字证书。

注：数字证书也称公钥证书（简称“证书”），由证书认证机构签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及扩展信息的一种数据结构。

3.6

路侧终端证书 road side unit certificate

用于智能汽车基础地图数据（3.1）传输过程中标识路侧终端身份信息的数字证书。

3.7

车载终端证书 on board unit certificate

用于智能汽车基础地图数据（3.1）传输过程中标识车载终端身份信息的数字证书。

4 传输场景

本文件规定的智能汽车基础地图数据传输场景如图1所示，包括以下四种情形：

a) 车载终端上传传感器数据到地图专有平台；
b) 地图专有平台分发产品数据到车载终端；
c) 地图专有平台分发产品数据到路侧终端；
d) 路侧终端分发产品数据到车载终端。

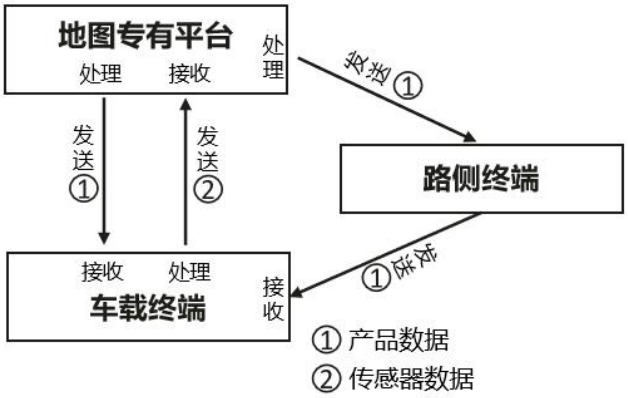

图 1 智能汽车基础地图数据传输场景示意图

5 基本要求

5.1 产品数据

产品数据传输时，应满足如下要求：

a) 由地图专有平台提供；
b) 采用完整性保护措施；
c) 采用技术措施确保数据传输的身份可信。

5.2 传感器数据

传感器数据传输时，应满足如下要求：

a) 经过安全处理；
b) 采用机密性和完整性保护措施；
c) 采用技术措施确保数据传输的身份可信。

6 安全保护方法

6.1 产品数据

6.1.1 数据安全处理

数据安全处理环节的保护方法包括：

——应利用GB/T 37092规定的密码模块对产品数据进行完整性计算；

——可利用GB/T 37092规定的密码模块对产品数据进行加密处理。

6.1.2 数据发送

数据发送环节的保护方法包括：

——应利用地图专有平台证书、路侧终端证书和车载终端证书完成地图专有平台、路侧终端与车载终端之间的身份认证；

——宜采用GB/T 38636规定的协议建立安全传输通道。

6.1.3 数据接收

数据接收环节应利用密码模块或安全芯片对接收数据进行完整性校验，对涉及6.1.1加密处理的接收数据应进行解密处理，密码模块或安全芯片应符合GB/T 37092或GM/T 0008相关要求。

6.2 传感器数据

6.2.1 数据安全处理

数据安全处理环节的保护方法包括：

——应采用国家认定的地理信息保密处理技术对传感器数据进行安全处理；

——传感器数据安全处理后，应利用密码模块或安全芯片进行完整性计算和加密处理，密码模块或安全芯片应符合GB/T 37092或GM/T 0008相关要求。

6.2.2 数据发送

数据发送环节的保护方法包括：

——应利用车载终端证书和地图专有平台证书完成车载终端和地图专有平台之间的身份认证；

——宜采用GB/T 38636规定的协议建立安全传输通道。

6.2.3 数据接收

数据接收环节应利用GB/T 37092规定的密码模块对接收数据进行解密处理和完整性校验。

7 证实方法

7.1 查验涉及智能汽车基础地图数据保密插件申请、批复和领取等实施记录，判断是否符合 6.2.1 的要求。

7.2 智能汽车基础地图数据传输的机密性保护、完整性保护以及身份可信，应按照 GB/T 43206 规定的技术测评要求，利用密码产品、网络和通信安全的测评指标进行检验。

参 考 文 献

[1] GB/T 44373—2024 智能网联汽车 术语和定义
[2] JT/T 1458—2023 营运车辆车路/车车通信（V2X）终端性能要求和检测方法
[3] 自然资源部办公厅关于推进地理信息保密处理技术研发和服务工作的通知〔自然资办发〔2021〕22号）
[4] 自然资源部关于促进智能网联汽车发展维护测绘地理信息安全的通知（自然资规〔2022〕1号）
[5] 自然资源部关于加快测绘地理信息事业转型升级更好支撑高质量发展的意见〔自然资发〔2023〕158号）
[6] 自然资源部关于印发《自然资源领域数据安全管理办法》的通知（自然资发〔2024〕57号）
[7] 自然资源部关于加强智能网联汽车有关测绘地理信息安全管理的通知（自然资发〔2024〕139号）