ICS 35.100.20
CCS M19

团　　体　　标　　准

T/KJDL 022—2024

车联网服务平台与车载终端交互安全技术要求

Technical Requirements for Security of Interaction between Internet of Vehicles Service Platform and Vehicle Terminal

2024－01－31 发布　　2024－03－01 实施

广州市空间地理信息与物联网促进会　　发 布

目　　次

前　　言 III
1 范围 1
2 规范性引用文件 1
3 术语、定义和缩略语 1
3.1 术语和定义 1
3.2 缩略语 2
4 系统架构 2
5 车联网服务平台及车载终端功能要求 3
5.1 车联网服务平台数据功能要求 3
5.2 车联网服务平台业务功能要求 4
5.3 车载终端数据采集功能要求 4
5.4 车载终端数据处理与存储功能要求 6
5.5 平台访问与数据安全 6
6 车联网服务平台及车载终端性能要求 7
6.1 智能网联服务平台总体性能要求 7
6.2 报警及响应时间要求 7
6.3 日志功能要求 7
6.4 智能网联车载终端整体性能要求 7
6.5 智能网联车载终端电气性能要求 7
6.6 智能网联车载终端数据接口性能要求 7
7 车联网服务平台与车载终端交互安全要求 7
7.1 网络与通信安全 8
7.2 车载终端操作系统安全 8
7.3 平台访问与数据安全 8
7.4 车联网服务平台与车载终端交互通信方式 9
7.5 车联网服务平台与车载终端交互接口命令 9
8 车联网服务平台安全技术要求 19
8.1 数据安全 19
8.2 系统安全 20
8.3 运维安全 20
8.4 通信安全 21
9 车载终端安全技术要求 22
9.1 硬件安全 22
9.2 通信协议与接口安全 22
9.3 车载终端操作系统安全 24
9.4 车载终端应用软件安全 25
9.5 车载终端数据安全 27
9.6 OTA 安全 28
附　录　A　（资料性）　车载终端设备典型逻辑图 29
附　录　B　（规范性）　V5 接口的安全过程 30
B.1 概述 30
B.2 安全基本元素说明 30

B.3 安全类数据结构总体要求 30
B.4 公钥证书格式 31
B.5 消息签名流程 31
B.6 加密消息流程 34
B.7 密钥协商 37

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。

本文件的某些内容有可能涉及专利，本文件的发布机构不应承担识别这些专利的责任。

本文件由深圳市交投科技有限公司提出。

本文件由广州市空间地理信息与物联网促进会归口。

本文件起草单位：深圳市交投科技有限公司、广东产品质量监督检验研究院、深圳市麦谷科技有限公司、移动通信国家工程研究中心、深圳广联数科科技有限公司、深圳联友科技有限公司、广东省电子商务认证有限公司、北京驭安科技有限公司、奇安信科技集团股份有限公司、高新兴科技集团股份有限公司、广州小鹏汽车科技有限公司、湛江市泰康投资有限公司、暨南大学、信阳师范大学、临沂大学、兰州理工大学、江苏大学、西安邮电大学、广东省车联网产业联盟、广州市空间地理信息与物联网促进会。

本文件主要起草人：庄杰、石光明、胡斌、刘化龙、沈剑、曹绍芬、许斯亮、李大成、朱宇翔、叶赛、李佐彪、曾少旭、刘志全、孔令晟、岳浩、赖成喆、冯霞、肖磊、成玉丹、谢孟思、李兰、陈木来、熊志欢、程洪圆、刘可儿、张嵩、梁宁宁、刘玉娟、杨文凤、肖薇薇、姚岚、黄斐然。

车联网服务平台与车载终端交互安全技术要求

1 范围

本文件规定了智能网联汽车服务平台与车载终端交互的系统架构、通信方式、接口命令规则及相关安全技术要求。适用于大湾区或各地级智能网联汽车运行监管系统的设计、建设和应用。相关智能网联平台与终端间交互及平台端数据、通信和安全规范可参考执行。

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 25068.4-2022 信息技术 安全技术 网络安全 第4部分：使用安全网关的网间通信安全保护
GB/T 25069-2022 信息安全技术 术语
GB/T 28458-2020 信息安全技术 网络安全漏洞标识与描述规范
GB/T 30276-2020 信息安全技术 网络安全漏洞管理规范
GB/T 30279-2020 信息安全技术 网络安全漏洞分类分级指南
GB/T 32960.2-2016 电动汽车远程服务与管理系统技术规范 第2部分：车载终端
GB/T 37025-2018 信息安全技术 物联网数据传输安全技术要求
GB/T 37376-2019 交通运输 数字证书格式
GB/T 37729-2019 信息技术 智能移动终端应用软件（APP）技术要求
GB/T 38674-2020 信息安全技术 应用软件安全编程指南
GB/Z 42885-2023 信息安全技术 网络安全信息共享指南
YD/T 3594-2019 基于LTE的车联网通信安全技术要求
YD/T 3751-2020 车联网信息服务 数据安全技术要求
YD/T 3752-2020 车联网信息服务平台安全防护技术要求
YD/T 3802-2020 电信网和互联网数据安全通用要求

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

监管平台 monitoring platform

具备智能网联汽车测试监管的数据存储、数据分析及处理、监控终端安装信息管理等功能的综合监管平台。

3.1.2

车载终端 on-board terminal

安装在智能网联汽车上，采集及保存整车和自动驾驶系统、网联系统等部件的关键数据并发送到监管平台的装置或系统。

3.1.3

接口 interface

在两个功能单元之间,由这两个功能单元的功能特性、物理互连特性、信号交换特性及其他适当特性界定的共享边界。

3.1.4

漏洞 vulnerability

车联网服务平台和车载终端中能够被威胁利用的弱点。

3.2 缩略语

下列缩略语适用于本文件。

AES：高级加密标准（Advanced Encryption Standard）

AS：应用服务器（Application Server）

CA：认证机构(Certificate Authority)

CAN：控制器局域网(Controller Area Network)

ECIES：椭圆曲线集成加密方案（Elliptic Curve Integrated Encryption Scheme）

GBA：用户认证（Generic Bootstrapping Architecture）

GCS：通用通信服务（Generic Communication Services）

GPS：全球定位系统（Global Positioning System）

HTTPS：超文本传输安全协议（Hypertext Transfer Protocol Secure）

IoV：车联网（Internet of Vehicle）

ITS：智能交通系统（Intelligent Transportation System）

LTE-Uu：LTE无线接口（Long Term Evolution-User Equipment and Evolved Node B）

MAC：介质访问控制（Medium Access Control）

OBU：车载终端（On-Board Unit）

OTA：远程固件升级（Over-The-Air）

PC5：设备间直接通讯的技术（Proximity Communication 5）

PDCP：分组数据收敛协议（Packet Data Convergence Protocol）

PHY：物理层（Physical Layer）

RLC：无线链路控制（Radio Link Control）

RSU：路边单元 （Road Side Unit）

SM2：国密SM2椭圆曲线公钥密码算法（Chinese National Cryptographic Algorithm SM2 Elliptic Curve Public Key Cryptography Algorithm）

SSL：安全套接层（Secure Sockets Layer）

SecOC：板端加密通讯（Security Onboard Communication）

TLS：传输层安全（Transport Layer Security）

UICC：通用集成电路卡(Universal Integrated Circuit Card)

V2I：车辆对基础设施通信（Vehicle-to-Infrastructure）

V2N：车辆对网络通信（Vehicle-to-Network）

V2P：车辆对行人通信（Vehicle-to-Pedestrian）

V2V：车辆对车辆通信（Vehicle-to-Vehicle）

V2X：车辆与一切通信（Vehicle-to-Everything）

3GPP：第三代合作伙伴计划（3rd Generation Partnership Project）

4 系统架构

系统架构应符合以下要求：

a) 监管系统包含监管平台和车载终端，如图 1 智能网联汽车测试监管系统架构所示；

b) 车载终端安装在智能网联汽车上，可通过 CAN 总线或车载以太网等采集车辆的运行数据和车载传感器的感知信息，同时应对采集到的数据进行本地存储和通过无线网络上传到远程监管平台；

c） 监管平台应部署在云端，应具备接收车载终端上传的数据，并进行数据的存储、分析、展示功能，应具备下发指令通知车载终端上传本地存储的历史数据功能。

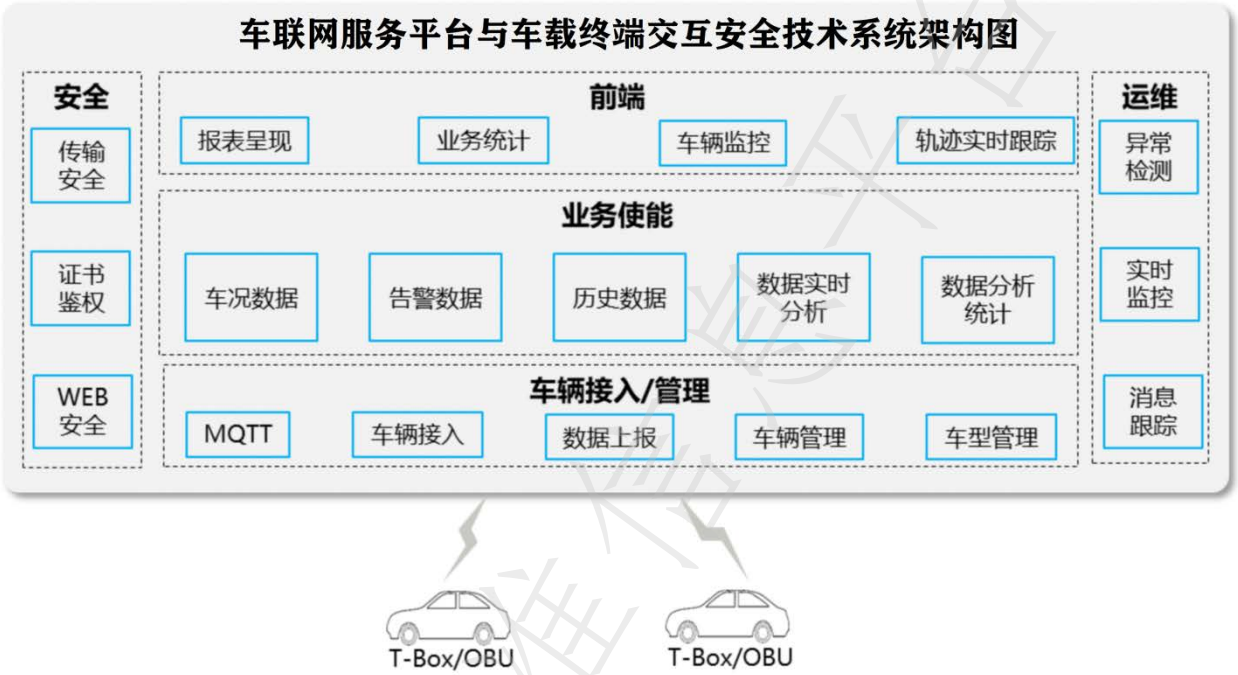


图1 系统架构图

5 车联网服务平台及车载终端功能要求

5.1 车联网服务平台数据功能要求

平台的数据功能要求包括数据接入、存储、显示功能，数据查询与报表导出功能，数据的开放功能。

5.1.1 数据的接入、存储、显示功能

数据的接入、存储、展示功能应符合以下要求：

a） 数据接入：监管平台应具备车载终端数据的接入功能，具备向车载终端提供注册、注销和鉴权管理的功能，车辆实时状态数据的接收频率≥ 1Hz，摄像头采集视频的帧率≥ 15fps，平台与车载终端交互数据应进行数据校验与加密；

b） 数据存储：监管平台应具备对接入车载终端上传数据的存储功能，应具备对存储的数据进行备份能力，防止数据丢失或其他异常发生，数据的存储期限应满足本文件第 7.3 条的相关要求；

c） 数据展示：监管平台应具备对接入数据进行处理与展示能力，满足对智能网联测试汽车安全监管的要求，数据的展示应包括实时数据的显示和历史数据显示。

5.1.2 数据查询与报表导出功能

数据的查询与报表导出功能应符合以下要求：

a） 平台应具备按测试企业、车牌、车辆 VIN 码、接管率、测试时间等单个条件或多个条件组合查询、导出数据功能；

b） 平台应具备按年、月、季、周、日生成相关数据报表并支持报表的展示功能，报表的数据项应包括车型数量、车辆数量、测试时长、测试里程、测试企业、测试时间、接管率等数据项。

5.1.3 数据的开放功能

数据的开放功能应符合以下要求：

a) 平台应具备数据开放功能，应提供统一的数据开放接口服务，为其它政府机构、第三方机构及企业提供数据服务，应具备数据开放的鉴权/授权能力；
b) 开放的数据应进行脱敏处理；
c) 开放的数据的传输需要进行加密传输。

5.2 车联网服务平台业务功能要求

5.2.1 基础业务功能

5.2.1.1 车辆管理

车联网服务平台应具备车辆管理功能，支持车辆注册、车辆查询、车辆事故上报信息记录、车辆历史轨迹查询、车辆日志查询等功能。

5.2.1.2 设施管理

车联网服务平台应具备设备管理功能，可实现点位信息展示、设备在线率统计、设备故障统计、路侧设备的分布展现、设备硬件异常告警、测试设备列表等功能。

5.2.1.3 测试场景管理

车联网服务平台应具备测试场景管理功能，支持测试场景地图信息展示、地图交互操作、测试监控视频、点位查询、场景库查询、场景库操作、关联场景、任务管理等功能。支持开展车路协同或自动驾驶测试活动。

5.2.1.4 系统管理

车联网服务平台应具备系统管理功能，包括用户管理、角色管理、菜单管理、部门管理、岗位管理、运行管理等功能。

5.2.2 核心业务功能

5.2.2.1 交通运行监测

应支持对路网状态、路网事件、路网车辆运行等的实时监测，可对全路网交通拥堵、交通事故、车辆异常等进行整体分析和快速发现。

5.2.2.2 车路协同服务

应支持在全时空动态交通信息采集与融合感知的基础上面向车路协同场景提供信息共享、预警提示、事件下发等服务，支持交通信息发布和道路协同管理等服务。

5.2.2.3 数字孪生展示

宜支持在全时空动态交通信息采集与融合感知的基础上基于数字孪生实现对物理交通世界的精准数字化映射,支持交通运行状态实时孪生及仿真推演等功能，从而帮助交通管理者进行实时、精准、智能的交通管理和信息发布，提升交通运行效率和安全性。

5.3 车载终端数据采集功能要求

5.3.1 车辆状态信息采集

车载终端应支持通过CAN或以太网口或串口采集智能网联汽车实时状态信息,数据的采集频率≥1Hz，采集的数据项最低要求应符合国家及所在地的智能网联汽车测试及示范相关管理的要求,采集的数据项宜包括：

a) 车辆的标识（车辆 VIN 和临时行驶车牌号）；
b) 车辆状态：0-离线，1-通电，2-启动，3-运行；
c) 驾驶模式：0-人工驾驶，1-自动驾驶；
d) 急停开关状态：0-关闭，1-启动；

e) 感知部件状态：激光雷达（0-无，1-正常，10-故障），毫米波雷达（0-无，1-正常，10-故障），摄像头（0-无，1-正常，10-故障），超声波雷达（0-无，1-正常，10-故障）；
f) 油门踏板开度：0%-100%；
g) 制动踏板开度：0%-100%；
h) 方向盘转角：0°-720°；
i) 方向盘转速：°/s；
j) 方向盘扭矩：N/m；
k) 档位：P，R，N，D；
l) 车速表读数：km/h；
m) 里程表读数：km；
n) 加速度：m/s^2；
o) 电机或者发动机转速： r/min；
p) 电池 SOC：0%-100%；
q) 续航里程：km；
r) 转向灯：0-关闭，1-左转，2-右转；
s) 制动灯：0-关闭，1-开启；
t) 夜灯：0-关闭，1-开启；
u) 近光灯：0-关闭，1-开启；
v) 远光灯：0-关闭，1-开启；
w) 雨刮：0-0 档，1-1 档，2-2 档，3-3 档，4-4 档，5-5 档；
x) 喇叭：0-不响，1-响；
y) 数据采集时间，时间戳精确到毫秒。

5.3.2 定位信息采集

车载终端应支持通过CAN口或以太网口或串口等方式采集车辆的定位信息，定位系统可是北斗/GPS/GLONASS/Galileo等，数据更新频率≥10Hz，定位精度应是厘米级以内，定位数据采集的数据项宜包括：

a) 经度，自车几何中心的经度；
b) 纬度，自车几何中心的纬度；
c) 高度，自车几何中心与路面的高度；
d) 航向角，自车航向角。

5.3.3 视频信息采集

车载终端应支持通过以太网口或视频数据接口采集视频数据，视频信息采集应满足以下要求：

a) 应具备对采集的视频数据进行压缩、存储和上传云平台功能，还应支持通过本地数据接口导出视频数据；
b) 应支持不低于 6 路视频的数据同时采集；
c) 视频分辨率应≥720P；
d) 本地存储视频帧率应≥25fps，上传云平台视频的帧率应≥15fps；
e) 视频中应显示当前的日期、时间（24 小时制）、定位、速度、车牌号(若无车牌号可空缺)等信息；
f) 视频采集编码格式应为 H.264 或 H.265。

5.3.4 V2X 网联信息采集

V2X（Vehicle to Everything）网联信息采集功能是指通过V2X通信技术，实现车辆与其他交通参与者（包括其他车辆、行人、道路基础设施等）之间的信息交互和共享。通过实时采集和传输各种交通信息，V2X系统能够提高道路安全性、交通效率以及驾驶体验。应当具备实时性，标准化，可靠性等功能要求。

车载终端应支持通过CAN口或以太网口采集V2X网联数据，数据采集应满足以下要求：

a) V2X 网联数据采集应包括 MAP、SPAT、RSM、RSI、BSM 五类数据，V2X 网联交互的数据编码要满足互联系统的交互要求；
b) 数据的采集频率应≥1Hz。

5.3.5 自动驾驶信息采集

车载终端应支持通过CAN口或以太网口采集网联汽车数据，采集频率应≥1Hz，采集数据应包括以下内容：

a) 目标 ID，每个目标有一个唯一的 ID；
b) 目标类别，机动车、非机动车、行人等；
c) 目标位置-经度，目标几何中心经度；
d) 目标位置-纬度，目标几何中心纬度；
e) 目标位置-高度，目标几何中心与路面的高度；
f) 目标长度，目标长度值，单位 cm；
g) 目标宽度，目标宽度值，单位 cm；
h) 目标高度，目标高度值，单位 cm；
i) 目标速度，单位 km/h；
j) 目标航向角，目标行进方向，传感器坐标系 x 轴正方向 顺时针旋转的弧度值；
k) 目标置信度；
l) 红绿灯状态：当前红绿灯允许直行、左转、右转的一个组合；
m) 车道线：一组坐标序列+车道线类型（包括虚线，实线，黄线，白线等）。

5.4 车载终端数据处理与存储功能要求

数据处理与存储应符合以下要求：

a) 连续场景数据与接管场景数据应分开保存在不同的文件目录下，接管场景数据应是连续场景数据的子集；
b) 连续场景数据及接管场景中的各类数据（如：车辆状态数据、定位信息数据、视频数据、V2X 网联数据和网联汽车数据等）应分开保存在不同的子目录中，但各类数据的采集时间应进行对齐；
c) 当发生人工接管时，车载终端应能快速把接管事件之前 30s 与接管之后 30s 的数据提出来，并快速把写入接管场景数据目录；
d) 车载终端采集到的数据应快速保存到车载终端的数据存储单元，连续场景的数据从采集到写入到存储单元时间应≤10s，接管场景数据从采集到写入存储单元的时间≤2s；
e) 连续场景数据本地保存时间应≥7d，事件数据本地保存应≥180d，内部介质储存满时，应具备储存数据的内部自动循环覆盖功能；
f) 车载终端的内部数据存储单元保存的数据应具备完整性及可读性；
g) 车载终端断电时，到保存在数据存储单元中的数据应不损坏、不丢失；
h) 车载终端应具有 USB Device 2.0 或以上接口读取功能；
i) 本地访问与读取终端上数据应通过口令验证，口令应在监管平台备案保存。

5.5 平台访问与数据安全

5.5.1 数据上传

数据上传应符合以下要求：

a) 车载终端应具有将实时/历史采集的数据上传到监管平台的功能；
b) 车载终端向监管平台上传数据的接口应符合监管平台的相关要求。

5.5.2 数据补发

数据补发应符合以下要求：

a) 当通信异常时，车载终端应将采集到的实时数据保存到内部存储介质中，等通信恢复正常后进行实时数据补发；

b） 数据补发时应按照数据的采集时间依次补发，先采集的数据先补发；
c） 当数据发送异常时应在 10s 内进行第一次补发，如补发失败应等待 1min 进行再补发，如果连接超过 10 次补发失败应停补发，并把数据保存在本地历史记录中。

6 车联网服务平台及车载终端性能要求

6.1 智能网联服务平台总体性能要求

平台总体性能应满足以下要求：
a） 应具备 7*24h 服务能力；
b） 服务等级协议应达到年服务障碍总时长≤24h，单次故障总时长≤30min；
c） 系统响应时间≤1s；
d） 系统的准确性≥99.9%；
e） 为保实时可靠运行，在系统最高运行负荷下应留有一定的冗余，具体冗余指标如下：
1） 备用 CPU 能力＞40%；
2） 备用内存容量＞30%；
3） 备用外存容量＞80%；
4） 备用 I/O 接口＞10%。

6.2 报警及响应时间要求

报警及响应时间应满足以下要求：
a） 平台优先保证报警信息及预警信息的处理、显示；
b） 平台收到报警信息或预警后到信息在平台上显示的时间应≤3s。

6.3 日志功能要求

系统的数据存储应满足以下要求：
a） 系统的业务数据存储时间应≥5y；
b） 系统的异常报警信息数据存储时间应≥5y；
c） 系统的日志数据存储时间应≥1y。

6.4 智能网联车载终端整体性能要求

整体性能应符合以下要求：
a） 启动时间：从上电到实时数据采集时间≤60s；
b） 防护等级：防护等级要求≥IP43；
c） 工作温度：-40℃～＋80℃；
d） 工作湿度：5%～95%；
e） 与监管平台服务器的通信时延：≤2s；
f） 与监管平台服务器的丢包率：≤0.1%。

6.5 智能网联车载终端电气性能要求

监控终端及外设的电气性能应符合GB/T 32960.2-2016中4.3.1规定的相关电气适应性能定义要求。

6.6 智能网联车载终端数据接口性能要求

数据接口性能应符合以下要求：
a） 具备满足≥720P、25fps 视频的数据采集传输接口，视频的数据采集传输接口可以是 RJ45、LVDS、GMSL 或 HDMI；
b） 具备≥1 路 CAN 接口；
c） 具备≥1 路以太网口；
d） 具备≥1 路 USB Host2.0 或以上标准接口。

7 车联网服务平台与车载终端交互安全要求

车联网服务平台网络安全防护是指采取安全防护措施，保障车联网服务平台网络安全。从安全防护内容上，车联网服务平台安全分为网络与通信安全、操作系统安全、平台访问和数据安全三个部分，其中网络与通信安全包括车内通信安全、车外通信安全、网络攻击监测与防御，操作系统安全包括访问控制、入侵防范、日志安全和外部连接安全，平台访问和数据安全包括平台访问控制、数据安全保护。

7.1 网络与通信安全

7.1.1 车内通信安全

a) 应对车内网络边界进行逻辑隔离或物理隔离；
b) 应对车辆内部网络进行区域划分，对跨越区域边界的数据流进行访问控制；
c) 车辆应对接入车内网络通信的设备进行身份校验；
d) 车内通信应采用 SecOC 等具备安全机制的 CAN 通信协议，具备加密和校验的车载以太网协议；
e) 车内通信数据传输应具备防重放攻击。

7.1.2 车外通信安全

车辆与外部通信时应使用高安全等级的通信协议，并对通信对象身份进行校验：

a) 车辆与服务平台的通信应采用虚拟专用网络，与公共网络隔离；
b) 车辆与其他车辆、路侧设备、服务平台进行通信时，应使用数字证书保证通信双方身份合法性和通信链路机密性；
c) 车辆与外部直接通信的关键设备应具备安全机制防止非授权的系统特权访问；
d) 车辆与外部通信的网络边界应具备访问控制机制；
e) 车辆应对发送的敏感个人信息实施保密性保护措施；
f) 车外通信接口应采用 TLS 加密通信协议，确保传输过程中数据的机密性和完整性；
g) 对数据接口的使用情况进行全面记录，包括访问时间、访问内容、访问者身份等，以便事后审计和安全溯源。

7.1.3 网络攻击监测与防御

a) 车辆在内、外部网络边界处应能识别网络攻击、恶意诊断数据发送、非法调试等异常行为，及时告警并进行处置；
b) 车载信息交互系统应能对网络攻击、恶意程序植入等异常行为进行安全监测，及时告警并进行处置；
c) 应采用访问控制技术，防止来自外部通道的数据对车辆数据的非法操纵、覆盖、清除或非法数据代码写入；
d) 车辆内部应具备监控手段，能够有效识别攻击行为，对攻击等异常行为能够产生安全事件，通过安全网络传输到平台，并安全存储相关日志。

7.2 车载终端操作系统安全

7.2.1 访问控制

a) 应具备访问控制机制，限制用户、进程等主体对文件、数据库等客体的访问；
b) 访问控制策略更改前需对操作用户进行身份鉴别；
c) 应及时删除默认账户、多余账户。

7.2.2 日志安全

a) 应具备对操作系统关键事件记录的日志功能，内容包括事件的时间、对象、操作等；
b) 车辆应采用安全技术手段，对存储在车内的安全日志进行保护，防止其被非授权修改和删除。

7.3 平台访问与数据安全

7.3.1 平台访问控制

a) 车辆与服务平台的通信，应实施身份认证；
b) 应采取措施检测和防止非特权用户获得对系统的特权访问。

7.3.2 数据安全

a) 应采取措施对数据进行安全存储；
b) 应对数据进行分级分类管理；
c) 数据处理者应当履行个人信息保护责任，遵循“告知同意义务和匿名化要求”，充分保护个人信息安全和合法权益。

7.4 车联网服务平台与车载终端交互通信方式

7.4.1 通信协议

a) 平台与车载终端网络层通信协议应支持 IPv4、IPv6；
b) 平台与车载终端传输层通信协议应支持 UDP、TCP；
c) 平台与车载终端安全传输协议宜采用 TLS、DTLS、TLCP，避免使用有安全漏洞的安全传输协议；
d) 平台与车载终端应用层通信协议宜采用 DNS、HTTP/HTTPS、MQTT、OCSP 等标准协议；
e) 平台应能够对接入的并发连接数和流量进行限制。

7.4.2 数据格式

a) 平台与车载终端传输数据，宜采用结构化数据；
b) 平台与车载终端传输数据的编码格式，可采用 OER、DER、JSON、XML 格式；
c) 平台与车载终端传输数据的字符编码，宜采用 UTF-8 编码。

7.4.3 数据安全加密

a) 平台与车载终端应采用数字证书技术保证通信双方的身份真实性，应采用国家许可的电子认证服务机构签发数字证书；
b) 平台与车载终端应采用密码技术保证通信过程中数据的完整性；
c) 平台与车载终端应采用密码技术保证通信过程中数据的机密性；
d) 平台与车载终端应采用技术手段对数据进行标识，避免历史数据的重放攻击；
e) 平台与车载终端宜采用国家商用密码算法，国家核准的密码产品或模块。

7.4.4 公私钥生成方法

a) 平台与车载终端应支持非对称密钥对的生成功能；
b) 非对称密钥对的生成宜采用国家商用密码算法；
c) 非对称密钥对的生成宜在国家核准的密码产品或模块内部随机产生；
d) 私钥需要在密码产品或模块外部传输或存储时，应采用加密技术保障其机密性。

7.5 车联网服务平台与车载终端交互接口命令

7.5.1 设备注册

7.5.1.1 接口功能

接口的功能应符合以下要求：
a) 车载终端绑定车辆时，第一次上电时应通过本接口进行注册；
b) 修改车牌码或设备重新绑定车辆时应通过本接口进行重新注册；
c) 监管平台收到注册请求后应马上处理过注册请求并把注册结果通过应答发送回给车载终端；
d) 车载终端发送注册请示后如超过 3min 没收到注册应答，应重新发送注册请求。

7.5.1.2 接口主题

接口的主题应符合以下要求：
a) 车载终端注册请求主题为：/vehicles-monitoring-sys/client/${terminal-id}/register/req；
b) 车载终端注册应答主题为：/vehicles-monitoring-sys/client/${terminal-id}/register/rsp。

7.5.1.3 请求数据

车载终端注册请求的业务数据应满足表1要求。

表1 车载终端注册请求数据

序号	名称	数据类型	是否可空	说明
1	enterpriseCode	String	否	测试或示范应用单位的企业代码，由监管平台分配
2	enterpriseKey	String	否	测试或示范应用单位的安全密码，由监管平台提供
3	vin	String	否	车辆VIN码
4	license	String	是	车牌号码，可是临时牌或正式牌照，如没车牌则应置为null
5	regTime	String	否	注册时间，格式为yyyy-MM-dd HH:mm:ss:SSS，精确到ms

7.5.1.4 应答数据

车载终端注册请求的应答返回值应符合表2的要求。

表2 车载终端注册返回值

返回值代码	异常值名称	说明
0	成功	表示注册成功
101	车载终端不存在	表示要注册的车载终端不存在
102	车载终端已被注册	表示车载终端已经被注册绑定到其它车辆
103	车辆不存在	表示要注册绑定到车载终端的车辆不存在
104	车辆重复绑定	表示注册要绑定的车辆已经被其它车载终端绑定

7.5.2 设备登入

7.5.2.1 接口功能

接口功能应符合以下要求：

a) 车载终端上电时应先登入，车载终端软件升级或检测到网联汽车软件升级后应重新登入；
b) 监管平台收到登入请求后应马上处理过注册请求，登入成功时登入成功后监管平台应返回 Token 车载终端；
c) 车载终端应登入成功后才能给监管平台上报其它数据，车载终端上报数据应带着 Token 上报数据，并且监管平台应校验 Token 是否合法；
d) Token 失效时车载终端应重新登入，并获取新的 Token；
e) 车载终端发送登入请示后如超过 5 分钟没收到注册应答，应重新发送登入请求。

7.5.2.2 接口主题

接口的主题应符合以下要求：

a) 车载终端登入请求主题为：/vehicles-monitoring-sys/client/${terminal-id}/login/req；

b) 车载终端登入应答主题为：/vehicles-monitoring-sys/client/${terminal-id}/login/rsp。

7.5.2.3 请求数据

车载终端登入请求的业务数据应满足表3要求。

表3 车载终端登入请求数据

序号	名称	数据类型	是否可空	说明
1	password	String	否	设备密码，在监管平台中设置
2	autoVersion	String	否	网联汽车软件版本号
3	autoUpdateTime	String	否	软件系统的更新时间，格式为：yyyy-MM-dd HH:mm:ss:SSS
4	autoReleaseTime	String	否	网联汽车软件的升级时间格式为：yyyy-MM-dd HH:mm:ss:SSS
5	terminalVersion	String	否	当前车载终端软件版本号
6	terminalUpdateTime	String	否	当前车载终端软件更新时间格式为：yyyy-MM-dd HH:mm:ss:SSS
7	terminalReleaseTime	String	否	当前车载终端软件发布时间格式为：yyyy-MM-dd HH:mm:ss:SSS

7.5.2.4 响应数据

车载终端登入请求的应答返回值应符合表4的要求。

表4 车载终端登入异常返回值

返回值代码	返回值名称	说明
0	成功	表示登入成功
101	密码错误	表示车载终端的登录密码不对

车载终端登入请示的应答数据应符合表5的要求。

表5 车载终端登入应答数据

序号	名称	数据类型	是否可空	说明
1	token	String	否	通信令牌
2	expiryTime	Integer	否	token失效时间，单位为分钟，车载终端应有失效前重新刷新token

3	loginTime	String	否	车载终端登录时间， 格式为yyyy-MM-dd HH:mm:ss:SSS 精确到ms

7.5.3 设备登出

7.5.3.1 接口功能

接口的功能应符合以下要求：

a) 车载终端不在上报数据时应通过本命令登出；

b) 车载终端登出后监管平台应注销 token。

7.5.3.2 接口主题

接口的主题应符合以下要求：

a) 请求主题为：/vehicles-monitoring-sys/client/${terminal-id}/logout/req；

b) 应答主题为：/vehicles-monitoring-sys/client/${terminal-id}/logout/rsp。

7.5.3.3 请求数据

车载终端登出请求的业务数据应满足表6要求。

表6 车载终端登出请求数据

序号	名称	数据类型	是否可空	说明
1	token	String	否	通信令牌token，每次登入时获到

7.5.3.4 响应数据

车载终端登出请求的应答返回值应符合表7的要求。

表7 车载终端登出返回值

返回值代码	返回值名称	说明
0	成功	表示登出成功
101	Token 不对	表示 token 不对

7.5.4 刷新 Token

7.5.4.1 接口功能

接口功能要求，车载终端应在Token失效前定期刷新Token有效期。

7.5.4.2 接口主题

接口的主题应符合以下要求：

a) 请求主题为：/vehicles-monitoring-sys/client/${terminal-id}/refresh-token/req；

b) 应答主题为：/vehicles-monitoring-sys/client/${terminal-id}/refresh-token/rsq。

7.5.4.3 请求数据

刷新Token请求的业务数据应满足表8要求。

表8 刷新 Token 请求数据

序号	名称	数据类型	是否可空	说明

1	token	String	否	表示要刷新的Token
2	vin	String	否	车辆的 VIN 码
3	license	String	是	车牌号码，可以是临时牌或正式牌照

7.5.4.4 响应数据

刷新Token请求的应答返回值应符合表9的要求。

表9 刷新 Token 返回值

返回值代码	返回值名称	说明
0	成功	表示刷新成功
101	Token 不对	/
102	Token 已失效	/

刷新Token应答数据应符合表10的要求。

表10 刷新 Token 应答数据

序号	名称	数据类型	是否可空	说明
1	token	String	否	通信令牌token，每次登入时获到
2	expiryTime	Integer	否	token失效时间，单位为分钟，车载终端应有失效前重新刷新token
3	refreshTime	String	否	刷新时间时间， 格式为yyyy-MM-dd HH:mm:ss:SSS精确到ms

7.5.5 车辆状态汇报

7.5.5.1 接口功能

接口功能要求,车载终端应实时上报车辆状态数据。

7.5.5.2 接口主题

接口主题要求,接口的主题应符合以下要求：

a) 请求主题为：/vehicles-monitoring-sys/client/${terminal-id}/status-report/req；
b) 应答主题为：/vehicles-monitoring-sys/client/${terminal-id}/status-report/rsp。

7.5.5.3 请求数据

车辆状态汇报请求数据规范见表11。

表11 车辆状态汇报请求数据

序号	名称	数据类型	是否可空	说明
1	token	String	否	通信令牌 token，每次设备登入时获到

2	vin	String	否	车辆的 VIN 码
3	license	String	是	车牌号码，可以是临时牌或正式牌照
4	workStatus	Integer	否	车辆状态：车辆离线-0，车辆通电-1，车辆启动-2，车辆运行-3
5	drivingMode	Integer	否	驾驶模式：人工驾驶-0，自动驾驶-1
6	mileage	Integer	否	累计里程，单位 1km
7	velocity	Double	否	车速，单位 0.01km/h
8	throttle	Integer	是	油门踏板开度：0-100%
9	acceleration	Double	是	加速度，单位 0.01m/s^2
10	brake	Integer	是	制动踏板开度：0-100%
11	steerAngle	Double	是	方向盘转角：[0°,720°]，单位为 0.01°
12	steerTorque	Double	是	方向盘扭矩，单位 0.01N*m
13	gear	String	否	档位：P，R，N，D
14	turnLamp	Integer	是	转向灯状态：关闭-0，左转-1，右转-2
15	bakeLamp	Integer	是	制动灯状态：关闭-0，开启-1
16	dippedLamp	Integer	是	近光灯状态：关闭-0，开启-1
17	highLamp	Integer	是	远光灯状态：关闭-0，开启-1
18	warnLamp	Integer	是	紧急告警灯光灯状态：关闭-0，开启-1
19	wiper	Integer	是	雨刮状态：关闭-0 ；1 档-1；2 档-2；3 挡-3；4 档-4；5 挡-5
20	horn	Integer	是	喇叭：不响-0，响-1
21	timestamp	Long	否	数据采集的时间戳，精确到 ms

刷新Token请求的应答返回值应符合表12的要求。

表12　刷新 Token 返回值

返回值代码	返回值名称	说明
0	成功	表示数据上报成功

101	Token 不对	/
102	Token 已失效	/

7.5.6 V2X 网联数据上报接口功能

7.5.6.1 接口主题

本接口用于支持V2X（Vehicle to Everything）通信中，车辆或其他交通参与者将其感知、状态及图等数据实时上传至V2X平台，以实现交通信息的共享与协同。

7.5.6.2 接口主题

接口主题应符合以下要求：

a) 请求主题为：/vehicles-monitoring-sys/client/${terminal-id}/v2xdata-report/req；
b) 应答主题为：/vehicles-monitoring-sys/client/${terminal-id}/v2xdata-report/rsp。

7.5.6.3 请求数据及响应数据

具体数据内容及编码方式应和接入系统相匹配。

7.5.7 实时视频查看及其他传感器数据

7.5.7.1 接口功能

接口功能要求，感知系统的状态汇报，应包括视觉感知、毫米波雷达、超声波雷达、激光雷达、定位IMU等感知设备的状态。

7.5.7.2 接口主题

接口主题应符合以下要求：

a) 请求主题为：/vehicles-monitoring-sys/client/${terminal-id}/perception-status/req；
b) 应答主题为：/vehicles-monitoring-sys/client/${terminal-id}/perception-status/rsp。

7.5.7.3 请求数据

车辆感知系统状态汇报请求数据应符合表13的要求。

表13 车辆感知系统状态汇报请求数据

序号	名称	数据类型	是否可空	说明
1	token	String	否	通信令牌 token，每次设备登入时获到
2	vin	String	否	车辆的标识（车辆的车架号）
3	license	String	是	车牌号码，可以是临时牌或正式牌照
4	cameras	List<Object>	是	视觉感知系统工作状态，这里的 Object 应符合表 18 视觉感知系统工作状态数据的要求
5	radars	List<Object>	是	毫米波雷达工作状态，这里的 Object应符合表19 毫米波雷达工作状态数据的要求
6	lidars	List<Object>	是	激光雷达工作状态，这里的 Object应符合表20 激光雷达工作状

				态数据的要求
7	ultrasonics	List<Object>	是	超声波雷工作状态，这里的Object应符合表21 超声波雷工作状态数据的要求
8	imus	List<Object>	是	Imu惯导组合系统工作状态，这里的Object应符合表22 IMU惯导组合系统工作状态数据要求
9	timestamp	Long	是	数据采集的时间戳，精确到 ms

视觉感知系统工作状态数据应符合表14的要求。

表14　视觉感知系统工作状态数据

序号	名称	数据类型	是否可空	说明
1	radarId	Integer	否	视觉感知设备 Id
2	radarPos	Integer	否	摄像头安装位置， 0-前挡风玻璃、1-车顶朝前、2-车顶朝左、3-车顶朝右、4-车顶朝后、5-前保险杠/前格栅、6-后挡风玻璃、7-A 柱朝前、8-A 柱朝后、9-B 柱朝前、10-B 柱朝后、11-C 柱朝前、12-C 柱朝后、13-后保险杠 、14-左外后视镜、15-右外后视镜、100-其它位置
3	workStatus	Integer	否	工作状态，0-故障、1-正常、2-遮挡

毫米波雷达工作状态数据应符合表15的要求。

表15　毫米波雷达工作状态数据

序号	名称	数据类型	是否可空	说明
1	radarId	Integer	否	毫米波雷达设备 Id
2	radarPos	Integer	否	毫米波雷达安装位置， 0-前向、1-左前角、2-右前角、3-左后角、-右后角、5-后向、100-其它位置
3	workStatus	Integer	否	工作状态，0-故障、1-正常、2-遮挡

激光雷达工作状态数据应符合表16的要求。

表16　激光雷达工作状态数据

序号	名称	数据类型	是否可空	说明
1	lidarId	Integer	否	激光雷达设备 Id
2	lidarPos	Integer	否	激光雷达安装位置 0-前向、1-车顶中间、2-车顶左侧中部、

				3-车顶右侧中部、4-左前角、5-右前角、6-左后角、7-右后角、100-其它位置
3	workStatus	Integer	否	工作状态，0-故障、1-正常、2-遮挡

超声波雷达工作状态数据应符合表17的要求。

表17　超声波雷达工作状态数据

序号	名称	数据类型	是否可空	说明
1	ultrasonicId	Integer	否	超声波雷达设备 Id
2	ultrasonicPos	Integer	否	超声波雷达雷达安装位置 0-左前中、1-左前角、2-左前、3-右前中 4-右前角、5-右前、6-左后中、7-左后角、8-左后、9-右后中、10-右后角、11-右后、100-其它位置
3	workStatus	Integer	否	工作状态，0-故障、1-正常、2-遮挡

IMU惯导组合系统工作状态数据应符合表18的要求。

表18　IMU 惯导组合系统工作状态数据

序号	名称	数据类型	是否可空	说明
1	ultrasonicId	Integer	否	惯导组合系统设备 Id
2	ultrasonicPos	Integer	否	惯导组合系统安装位置 0-后备箱、1-车内前部、2-车内中部、3-车内后部、100-其它位置
3	workStatus	Integer	否	工作状态，0-故障、1-正常、2-遮挡

车辆感知系统状态上报请求的应答返回值应符合表19的要求。

表19　车辆感知系统状态汇报返回值

返回值代码	返回值名称	说明
0	成功	表示数据上报成功
101	Token 不对	/
102	Token 已失效	/

7.5.8　历史视频文件查询

7.5.8.1　接口功能

按照音视频类型、通道号、报警类型和起止时间等组合条件从终端中查询历史视频文件列表。

7.5.8.2　接口主题

接口主题要求应符合以下要求：
请求主题为：/vehicles-monitoring-sys/client/${terminal-id}/video-file-query/req；
应答主题为：/vehicles-monitoring-sys/client/${terminal-id}/video-file-query/rsp。

7.5.8.3 请求数据

表20 历史视频文件查询请求数据

序号	名称	数据类型	是否可空	说明
1	token	String	否	通信令牌 token，每次设备登入时获到
2	vin	String	否	车辆的 VIN 码
3	license	String	是	车牌号码，可以是临时牌或正式牌照
4	channel	Integer	否	摄像头通道号，从 1 开始，0 表示所有通道
5	beginTime	Long	否	查询开始时间戳
6	endTime	Long	否	查询结束时间戳
7	videoType	Integer	是	音视频类型，0-音视频 1-音频 2-视频,默认名为 0
8	streamType	Integer	是	0:所有码流，1:主码流，2:子码流，默认为 0
9	memoryType	Integer	是	0:所有存储器，1:主存储器，2:灾备存储器，默认为 0

7.5.8.4 响应数据

表21 历史视频文件查询异常返回值

返回值代码	返回值名称	说明
0	成功	表示查询成功
101	Token 不对	/
102	Token 已失效	/
103	参数错误	/

表22 历史视频文件查询响应数据

序号	名称	数据类型	是否可空	说明
1	total	Integer	否	音视频文件总数，无符合条件的音视频文件,置为 0
2	fileLists	Object	是	音视频文件列表

表23　历史视频文件查询响应音视频文件列表内容

序号	名称	数据类型	是否可空	说明
1	channel	Integer	否	摄像头通道号
2	beginTime	Long	否	音视频文件录制开始时间戳
3	endTime	Long	否	音视频文件录制结束时间戳
4	videoType	Integer	是	音视频类型，0-音视频 1-音频 2-视频,默认名为 0
5	streamType	Integer	是	0:所有码流，1:主码流，2:子码流，默认为 0
6	memoryType	Integer	是	0:所有存储器，1:主存储器，2:灾备存储器，默认为 0
7	fileSize	Integer	是	音视频文件大小，单位：BYTE
8	format	Integer	否	音视频文件格式：0-MP4 1-MOV 2-WMV 3-FLV 4-TS 5-AVI 6-MKV 7-MP3 8-WAV 9-AAC 10-FLAV

8　车联网服务平台安全技术要求

8.1　数据安全

8.1.1　数据采集安全

a）　对车载终端信息、车辆状态信息、车辆定位信息、实时视频信息、V2X 网联信息和自动驾驶信息等数据的采集，应明示采集的范围和使用目的，必须得到数据所有者的授权；
b）　数据采集中使用的接口、工具、方法、传输、数据存储等整个过程公开透明，必须记录完整的日志，可以回溯和审计；
c）　数据采集必须在身份认证通过并被授予权限后才能执行。

8.1.2　数据存储安全

a）　对车辆状态信息、车辆定位信息、V2X 网联信息等敏感字段的存储应进行加密。存储的数据必须经过身份验证和授权才能访问；
b）　存储的数据使用完毕或者时限达到之后，必须完全销毁；
c）　对车辆状态、实时视频、历史视频等信息中涉及的人脸、车牌等敏感数据进行脱敏或者使用匿名化的技术处理和存储。

8.1.3　数据传输安全

a）　数据传输前必须身份认证和授权；
b）　敏感数据应该脱敏或加密后才能传输。

8.1.4　数据共享安全

a）　数据共享必须得到数据所有者的授权，明确共享对象、时间、地点、内容、方式、用途，必须有日志记录；

b) 数据共享通道必须使用身份认证和加密技术；
c) 对 V2X 网联信息、自动驾驶信息、车辆状态信息、车辆定位信息共享和公开时，应采用区块链等技术保证数据的访问授权、透明、不可篡改、可回溯。

8.1.5 数据跨境安全

必须对需要跨境传输的数据进行安全风险评估，遵守国家数据出境的相关规定。

8.2 系统安全

网络安全漏洞是指网络产品和服务在需求分析、设计、实现、配置、测试、运行、维护等过程中，无意或有意产生的、有可能被利用的缺陷或薄弱点。这些缺陷或薄弱点以不同形式存在于网络产品和服务的各个层次和环节中，一旦被恶意主体所利用，就会对网络产品和服务的安全造成损害，从而影响其正常运行。

车联网中漏洞可分为系统漏洞和网络服务漏洞，其中系统漏洞主要发生在车载硬件、软件等方面，网络服务漏洞主要发生在网络通信、车载服务等多方面，涉及车辆控制系统、信息娱乐系统、远程控制系统、车联网平台等多个模块，这些漏洞可能导致车辆失控、数据泄露、隐私侵犯、恶意攻击等严重后果。

8.2.1 系统漏洞及补丁

车联网系统漏洞及补丁可参考以下步骤：

a) 漏洞发现与报告：分析车联网系统硬件、软件的运行过程，漏洞发现者通过人工或者自动的方法对漏洞进行探测、分析正是漏洞存在的真实性，并由漏洞报告者将获得的漏洞信息向漏洞接收者报告；
b) 漏洞接收与验证：通过相应途径接收到漏洞后，对漏洞信息进行技术验证；
c) 针对漏洞设计补丁：对于验证后确定存在的漏洞，需要制定相应的补丁，可以从外部厂商或自行设计。在设计补丁时应考虑兼容性、稳定性等因素；
d) 实施补丁：根据不同场景下的具体情况实施补丁，为车联网系统和网络服务提供安全保障；
e) 审查补丁：对补丁的设计和实施过程进行审查，并跟踪检测漏洞修复情况，确保补丁的有效性和安全性。

8.2.2 网络服务漏洞及补丁

车联网网络服务漏洞及补丁可参考以下步骤：

a) 漏洞分类分级：将车联网网络服务漏洞进行分类，例如代码问题、配置错误、环境问题和其他；同时对漏洞进行分级，通过技术分级与综合分级，将漏洞分为超危、高危、中危和低危四个等级，以便更好地进行管理和处理。
b) 漏洞评估：对于每个漏洞进行评估，确定其危害程度和影响范围。可以使用一套漏洞评估模型或标准，来评估漏洞的严重性。
c) 补丁设计与实施：对于每个漏洞，制定相应的补丁措施。补丁的设计应该是针对具体漏洞的，应包括修复方法和步骤，并确保补丁的有效性和稳定性。在实施补丁时，应制定详细的计划和过程，包括测试和验证的步骤，确保补丁的顺利安装和系统的正常运行。
d) 漏洞披露与通知：制定漏洞披露和通知的标准和程序，确保漏洞能够及时被安全研究人员或相关方发现并反馈。同时，及时通知相关用户和利益相关者，并提供相应的解决方案和补丁。
e) 漏洞管理与更新：建立漏洞管理和更新的机制，包括定期进行漏洞扫描和审查，跟踪最新的漏洞信息和威胁情报，并持续开发和发布补丁，以确保车联网系统的持续安全。

8.3 运维安全

a) 平台系统必须达到前文所述的性能要求，系统设计不能为了性能而牺牲安全要求，也不能因为安全要求而影响平台性能。
b) 对任何功能的使用、操作等都必须认证、授权和记录日志。所有功能的认证、授权必须分层分级，例如，用户角色的权限分级有超级管理员、维护管理员、普通用户等。

c) 必须设定负责运维管理的角色，可以根据运维内容授予权限，只有通过认证和授权的用户才能实施运维。
d) 必须记录完整的运维日志，包括运维人员、时间、内容、地点、运维方法等，运维人员不能修改、删除运维日志。
e) 对平台关键功能操作、关键数据处理、系统到达告警阈值、识别出恶意攻击等，平台必须触发告警，并记录日志。
f) 用户管理中必须有安全审计管理员的角色，负责分析和审计系统运维日志。

8.4 通信安全

8.4.1 身份认证

通信安全身份认证应满足以下要求：
a) 用户身份验证；
b) 服务平台身份验证；
c) 双向身份认证；
d) 多因素身份验证；
e) 令牌和密钥管理；
f) 安全通信协议；
g) 强密码策略；
h) 防护措施：包括防火墙、入侵检测系统、加密和网络隔离等；
i) 错误处理：包括账户锁定策略、密码重置等。

8.4.2 通信传输安全

本项要求包含但不限于以下项目：
a) 应满足 GB/T 37025-2018 的完整性要求；
b) 应选择强密码学基础的加密算法,如 AES 或 RSA,以防数据在传输过程中被未授权的个体获取；
c) 应实施安全的密钥生成和分发机制，周期性地更新密钥以应对安全漏洞和密码学攻击；
d) 应引入时间戳或单次令牌来防止消息重放攻击，实施过期机制，限制过时数据的使用；
e) 应确保车联网服务平台与车载终端之间数据传输的高可用性，维护数据传输的稳定性和及时性。

8.4.3 应用通信安全

应用通信安全要求包含但不限于以下条款：
a) 应满足 GB/T 25068.4-2022 中的安全控制要求；
b) 信息共享应满足 GB/Z 42885-2023 中的安全性要求；
c) 应采取适当的隔离措施，确保车载终端之间以及与服务平台之间的通信数据相互隔离，并实施网络分段，将不同安全级别的通信数据隔离开来；
d) 应实施细粒度的访问控制策略，限制车载终端和服务平台之间的数据访问，使用最小权限原则，确保每个实体只能访问其所需的信息；
e) 应记录所有与通信相关的事件，确保全面的安全日志记录，并定期审查日志，检测潜在的安全威胁和异常行为；
f) 应部署异常行为检测系统，监视车载终端和服务平台之间的通信，以便及时发现异常行为，且实施自动响应机制，对异常行为采取及时的安全措施；
g) 应提供安全培训，确保车载终端和服务平台的操作人员了解通信安全的最佳实践，定期进行安全意识提升活动，强调对潜在风险的警觉。

8.4.4 通讯安全防护

车联网平台必须具备检测和防护能力，可以支持DDOS、仿冒接入、伪造指令、OTA防护、诊断及控制指令防护等入侵检测和防护。

9 车载终端安全技术要求

9.1 硬件安全

9.1.1 车载终端硬件安全要求

a) 必须提供车载终端开启的接口功能说明和使用规范，不应开启未经说明的接口。任何接口接入访问必须认证和授权；
b) 车载终端必须禁用未经声明的硬件接口，不存在隐藏的后门或接口；
c) 使用的关键芯片（例如：处理器、传输敏感信息的芯片、安全芯片等）应避免暴露管脚；
d) 车载终端要有外部保护措施，例如防护罩等，避免外部环境对关键硬件功能的影响；
e) 车载终端的电路板及芯片不能暴露用以标注端口和管脚功能的可读丝印。

9.2 通信协议与接口安全

9.2.1 外部通信安全

a) 与外部通信必须身份认证、授权，并记录认证授权的关键事件，保存日志；
b) 外部传输通道必须采用 SSL、TLS 等加密技术；
c) 车辆终端必须提供可以主动终止与外部通信连接的机制；
d) 车载终端必须支持指令注入、中间人劫持等入侵检测和防护功能。

9.2.2 内部通信安全

a) 车内通信数据交互应当采用轻量型加密技术和完整性校验技术；
b) 车内通信应当认证授权。

9.2.3 V2X 通信安全

9.2.3.1 概述

V2X通信系统支持车-车(V2V)应用、车-路 (V2I)应用、车-网 (V2N)应用和车-人(V2P)应用，利用这些应用可向用户提供诸如道路安全、交通效率提升和信息娱乐等各类业务。

V2X通信有两种操作模式， 基于PC5的V2X通信和基于LTE-Uu的V2X通信。 基于LTE-Uu的操作模式可以是单播或广播方式。V2X设备可以分别使用这两种操作模式进行接收和发送。

9.2.3.2 V2X 车联网通信安全架构

V2X 通信安全包括承载安全(PC5 安全或 LTE-Uu 安全)和 V2X 应用安全两部分，表 24 描述了基于 PC5 的 V2X 安全架构，表 25 描述了基于 LTE-Uu 的 V2X 安全架构。

表24 基于 PC5 的 V2X 通信安全协议架构

V2X应用安全	V2X应用
	V2X网络层
PC5安全	PDCP
	RLC
	MAC
	PHY

表25 基于 LTE-Uu 的 V2X 通信安全协议架构

V2X应用安全	V2X应用

LTE-Uu安全	PDCP
	RLC
	MAC
	PHY

图2给出了基于LTE的车联网应用层通信安全架构，功能如下：

a) V2X 应用安全子系统：位于 V2X 车辆、V2X 路边单元、V2X 服务提供商的应用服务系统中负责为 V2X 应用提供通信安全的功能实体。

b) V2X 应用：位于 V2X 车辆、V2X 路边单元、V2X 服务提供商的应用服务系统中需要 V2X 应用通信安全的功能实体。

c) V2X 安全管理实体：负责对 V2X 应用安全子系统进行安全配置和安全数据供应的功能实体，例如，注册、授权、密钥供应和证书颁发等功能实体。

d) V2X 应用安全服务：位于 V2X 应用安全子系统中，与 V2X 应用进行交互以完成消息签名、验证、加密、解密等操作，与 V2X 安全管理实体进行交互完成密钥写入，证书申请与写入等操作。

e) 安全环境：存储重要的安全数据，例如，CA 证书、公私钥和加/解密密钥等；为安全服务实体提供重要的安全计算服务，如数字签名、数据加密和解密等。

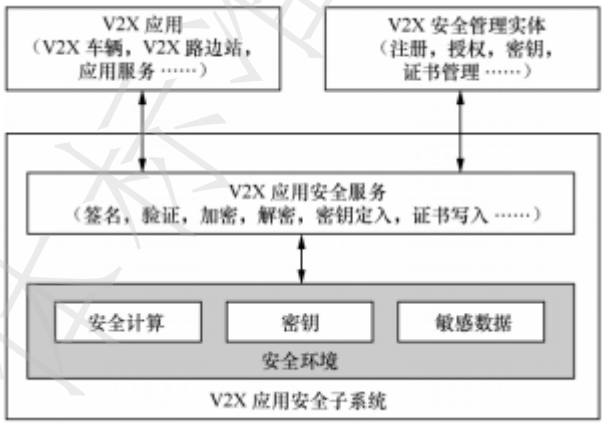


图2　V2X 应用层通信安全架构

9.2.3.3　通用安全要求

a) 当 V2X 设备使用支持 V2X 通信的 E-UTRAN 提供的服务时，3GPP 网络应提供运营商授权 V2X 设备进行 V2X 通信的方法；

b) 3GPP 网络应提供一种运营商授权 V2X 设备在未获得支持 V2X 通信的 E-UTRAN 服务时进行 V2X 通信的方法；

c) 3GPP 网络应提供一种授权 V2X 设备使用车到网络通信服务的方法；

d) 3GPP 网络应保护 V2X 设备传输的完整性；

e) 根据监管机构的要求，3GPP 网络应保护 V2X 设备的匿名性和隐私性，保证 V2X 设备在 V2X 应用所要求的某一段时间之内不应被其他终端追踪或识别；

f) 根据监管机构的要求，3GPP 网络应保护 V2V/V2I 通信终端的匿名性和隐私性，保证 V2X 设备不应被未经监管机构或用户授权的一方在该区域追踪；

g) 系统应支持使用国产商用密码算法；

h) 系统应支持安全传输通道，如 https 等；

i) 系统应支持敏感信息的安全存储。

9.2.3.4 网元的安全要求

9.2.3.4.1 V2X 设备

对于 PC5通信，V2X设备应支持基于证书的应用层安全机制，具体见V5 接口安全。对于Uu通信，V2X设备应支持LTE通信安全机制，包括基于EPS-AKA的双向认证、空口加密和信令消息的完整性保护，其中空口加密由V2X设备和LTE网络协商决定是否启用。对于基于MBMS的Uu通信，V2X设备可以不支持空口加密功能。V2X 设备应同时支持基于证书的应用层安全机制。为保护用户隐私，V2X 用户侧设备(如车辆)可在应用层进行匿名化处理，具体见V5接口安全。当应用层指示应用层 ID 变化时，V2X 设备应随机地改变自己的层二ID。V2X 设备应支持使用安全运行环境、安全单元或安全处理器等对敏感信息(如密钥、证书等)的保护。

9.2.3.4.2 V2X 控制功能

V2X 控制功能应支持YD/T 3594—2019的7.2章定义的安全机制以保护V3接口的安全。

V2X 控制功能应支持YD/T 3594—2019的7.1章定义的安全机制以保护与其他网元接口的安全。

9.2.3.4.3 V3 接口安全要求

a) V2X 设备和其 HPLMN 的 V2X 控制功能应支持双向认证。
b) V2X 控制功能和 V2X 设备之间的配置数据传输应支持完整性保护。
c) V2X 控制功能和 V2X 设备之间的配置数据传输应支持机密性保护。
d) V2X 控制功能和 V2X 设备之间的配置数据传输应支持抗重放攻击。
e) V3 接口上的 V2X 设备身份应支持机密性保护。

9.2.3.4.4 V4 接口安全要求

a) V2X 网络实体应能认证所接收到的数据通信的发送方，即 V2X 控制功能和 HSS 应能认证对方。
b) V2X 网络实体之间(即 V2X 控制功能和 HSS 之间)的数据传输应受完整性保护。
c) V2X 网络实体之间(即 V2X 控制功能和 HSS 之间)的数据传输应受机密性保护。
d) V2X 网络实体之间(即 V2X 控制功能和 HSS 之间)的数据传输应支持抗重放攻击。

9.2.3.4.5 V5 接口安全要求

a) 消息接收方应支持认证消息发送方，V2X 设备上的 V2X 应用可能既是消息发送方，又是消息接收方 V2X 应用之间传输的数据应支持完整性保护。
b) V2X 应用之间传输的数据可支持机密性保护。
c) V2X 应用之间传输的数据应支持抗重放攻击。

9.2.3.4.6 MB2 接口安全要求

V2X业务使用GCSE的MB2接口,其安全要求如下：

a) BM-SC 所处安全域的节点与 GCS AS 所处安全域的节点之间应进行双向认证。
b) BM-SC 和 GCS AS 之间 MB2-C 接口的信令消息应支持完整性和机密性保护。
c) BM-SC 和 GCS AS 之间的 MB2-U 接口的用户面消息应支持完整性保护。
d) BM-SC 可能对 GCS AS 发起的消息进行接入控制。
e) CS AS 可能对 BM-SC 发起的消息进行接入控制。

9.2.3.5 V5 接口的安全过程

V5接口的安全过程参见附录B。

9.2.3.6 其他接口的安全过程

其他接口的安全过程参见YD/T 3594—2019的第7部分。

9.3 车载终端操作系统安全

9.3.1 操作系统安全

a) 禁止 ROOT 等超级用户直接登录，只有授权用户才能获得特权权限；
b) 必须提供对用户角色或者其他管理对象分层分级的安全机制，实现精准的访问控制；
c) 禁止不必要的服务（例如：FTP 服务等），禁止非授权的远程接入服务，使用安全协议和认证方式限制远程访问；
d) 必须定期清理、删除或禁用不再需要的用户账号、共享目录或者其他历史授权配置；
e) 必须对外部通信、内部通信、认证授权等有完备的日志记录，日志只有特定的用户角色能修改删除；
f) 必须对系统运行状态、应用软件的使用、外部网络恶意连接等实时监测，有异常能触发告警，并能自动采取应对措施；
g) 必须对关键事件、关键操作、关键配置变更、安全事件、校验成功或失败等事件进行管理，记录事件、分析行为和审计日志；
h) 对开发者调试接口进行管控和定期审计，禁止非授权访问；
i) 必须提供安全补丁维护更新机制，不应存在由权威漏洞平台公开发布 3 个月及以上且未经处置的高危安全漏洞；
j) 必须提供阻断应用软件以高敏感权限（例如：ROOT 权限、删除日志等）运行或越权运行的机制。

9.4 车载终端应用软件安全

9.4.1 应用软件基础安全

车载终端的应用软件需要确保应用程序不易受到恶意攻击、数据泄漏和其他安全威胁，确保安全性和稳定性，基础安全技术要求包括但不限于：

a) 进行身份认证和访问控制，确保只有经过授权的用户能够访问应用程序，包括使用强密码策略、多因素认证以及明确定义的访问控制列表；
b) 保护应用程序中存储的敏感数据，包括数据加密、数据备份、数据遮蔽（数据脱敏化）、数据归档和灾难恢复等措施；
c) 在应用软件的开发和维护过程中采用安全编码实践，以减少代码漏洞和弱点的存在；
d) 进行定期的安全测试和漏洞扫描，以发现和纠正应用程序中的潜在漏洞，包括静态代码分析、动态应用程序安全测试（DAST）和漏洞扫描工具的使用；
e) 确保应用程序的组件和依赖项保持最新，以修复已知的漏洞和弱点，定期进行安全更新和维护，包括操作系统、数据库、第三方库和框架等；
f) 培训开发人员、管理员和终端用户，使其了解应用软件基础安全的最佳实践，并能够识别和应对安全威胁；
g) 建立和执行安全政策和流程，以确保应用软件的安全性符合法规和标准的要求；
h) 建立安全审计和监测机制，以检测和应对潜在的安全威胁和入侵，包括实时监控、事件日志记录和安全信息与事件管理（SIEM）系统。

9.4.2 应用软件代码安全

车载终端的应用软件代码安全技术要求包括但不限于：

a) 宜采取反编译防护、反盗版防护等措施防止被破解、篡改或二次打包，保护源代码安全；
b) 所引用或包含第三方代码或开源代码，应确保第三方代码或开源代码安全性，应对已公布的安全漏洞及时更新；
c) 代码中不应存在已公布的高危风险漏洞；
d) 应禁止内部组件被外部程序调用，如需供外部调用，应检查调用者是否符合访问控制机制。

9.4.3 应用软件访问控制

车载终端的应用软件访问控制技术要求包括但不限于：

a) 应对授权访问的内容严格访问控制，不应有超出授权范围的访问，当第三方通过应用软件访问被保护的用户数据时，应先获得用户许可或同意；
b) 未经用户许可，应用软件不应修改终端资源配置，不应修改和删除终端数据；

c) 未经用户许可，应用软件不应访问终端信息（如设备信息、地理位置、联系人信息、通讯记录等）和终端资源（如发送短信、拨打电话、连接网络、拍照、录音、调用其他应用等）；
d) 不应拦截或存留用户敏感或隐私信息，如用户支付密码等；
e) 根据业务需要，依据权限互斥的原则，保证用户、权限合理对应关系，避免任何可能产生安全问题的权限分配方式或结果；
f) 被用户赋予或修改权限后，宜不需重启系统，应用软件相应的权限即可生效；
g) 不应拦截或屏蔽系统或设备产生的用户提示信息或安全警告；不应在安全警告显示前，利用信息或警告误导或欺骗用户；不应模拟系统信息或安全警告误导用户。

9.4.4 应用软件运行安全

车载终端的应用软件的运行安全需要重点从以下方面保障，包括但不限于：
a) 应用软件发布前去除所有与调试和测试相关的代码、配置、文件等。
b) 应用程序的安全配置信息以可读的形式输出，以支持审计。
c) 对重要的配置信息进行安全保护。
d) 删除用户可访问的源码中的注释，避免用户通过逆向或者直接获取网页源代码方式获取源代码注释。
e) 如果应用软件部署在客户端，例如移动 APP,宜使用混淆、签名、加固等措施防止逆向获取源代码。
f) 及时删除服务器上不需要的应用程序和系统文档。
g) 关闭服务器上不需要的服务。
h) 建议禁止自动目录列表功能。如果必须开启目录列表功能，则需对目录下的文件进行详细检查，确保不包含敏感文件。
i) 确保软件运行服务器的系统组件均为相对安全的稳定版本，并安装了该版本的所有补丁。避免使用存在已知漏洞的组件版本。

9.4.5 应用软件通信安全

车载终端的应用软件通信安全性要求包括但不限于：
a) 应用软件运行过程中，如果有来电、语音、视频请求时，应用软件应自动切换到后台，优先处理通讯请求，并在处理完毕后可正常恢复，继续原来的功能；
b) 应能处理网络连接中断，并提示用户连接中断的情况；
c) 网络异常（如通讯切换或中断）时，应用软件应能及时将异常情况通报给用户；
d) 网络通信超时，应用软件应发送超时提示信息给用户；
e) 当不再需要使用网络连接时，APP 应及时关闭或断开连接，减少对网络资源的占用；
f) 当用户在公共免费网络环境中（如商场、咖啡馆等）使用应用软件,宜提醒用户注意数据安全。

9.4.6 应用软件日志安全

车载终端的应用软件日志记录了系统运行状况，通常包括软硬件故障、系统重要事件等。日志记录的设计和实现需从以下方面提升安全性，包括但不限于：
a) 保护日志文件：
   1) 对日志文件进行安全存储。
   2) 消息摘要算法以验证日志记录的完整性。
b) 在可信任的环境中执行日志记录操作。
c) 将日志记录作为集中化程序框架的一部分。
d) 在每个日志条目中增加精确的时间戳，同时确保时间戳的可靠性。
e) 对每个重要的行为都记录日志：
   1) 确保系统在发生重要安全事件时创建日志。
   2) 通常重要安全事件包括：重要数据更改、认证尝试（特别是失败的认证）、失败的访问控制、失效或者已过期的会话令牌尝试、系统例外、管理功能行为、失败的后端 TLS 链接、加密模块的错误。

f) 对日志记录进行完善的异常捕获处理，确保即使日志记录过程发生异常，日志记录仍然能够继续正确的执行。
g) 对日志中的特殊元素进行过滤和验证。确保日志记录中的不可信数据，不会在查看界面或者运行软件时以代码的形式被执行。
h) 采取安全措施防止攻击者写任意的数据到日志中。
i) 避免在日志中保存敏感数据。

9.5 车载终端数据安全

9.5.1 数据采集安全

a) 应制定数据采集规则，规范数据采集渠道、数据格式、采集流程和采集方式，并定期根据规则在业务系统中执行数据采集合规性审查。
b) 建立组织机构的数据质量管理体系，保证数据采集过程中数据的准确性、及时性和完整性。
c) 应对直接采集或者从其他途径获得的数据负有同等的保护责任和义务，对数据采集环境（如渠道）、采集设施和采集技术采取必要的安全管控措施。
d) 应加强数据采集设备安全防护工作，采取安全防护手段防止针对数据采集设备的网络攻击，严格落实数据采集设备的访问控制。
e) 应严格遵守数据采集规则，网站、应用程序涉及采集数据的功能设计应同隐私政策保持一致，同步调整。
f) 通过在线方式进行敏感信息采集时，应使用加密传输以保障用户在线提交信息的安全性。
g) 应明确数据采集过程中用户数据的知悉范围和安全控制措施，采取相应手段确保采集过程中的数据不被泄露。
h) 在停止运营产品或服务、用户终止服务等情况时，应立即停止对数据的采集。

9.5.2 数据存储安全

a) 应支持实现数据存储的保密性。
b) 应能够检测到数据在存储过程中完整性收到破坏，防止数据被篡改、删除和插入等操作。在数据完整性遭到破坏时，应提供可察觉的告警信息。
c) 应按照数据访问权限管理制度和数据存储安全策略，对车联网服务平台的不同数据应用相应的访问控制策略，确保非授权用户或应用程序不能访问数据。
d) 应明确数据备份的规范和操作规程，明确数据备份周期、备份方式、备份地点、数据恢复性验证机制等内容，保障数据的可用性和完整性。一旦发生数据丢失或破坏，可以利用备份来恢复数据。
e) 应将数据存储系统及相关数据处理和传输设备部署在安全域内，不直接提供公共互联网访问。

9.5.3 数据传输安全

a) 应采用技术措施保证数据传输的保密性（如鉴别信息（指用于鉴定用户身份是否合法的信息）、其他敏感数据等）。
b) 应能够检测到数据在传输过程中完整性收到破坏，并能够在检测到完整性遭到破坏时采取必要的措施恢复或重新获取数据。
c) 应区分安全域内、安全域间等不同数据传输业务场景，并参考 YD/T 3751-2020 中数据分类及敏感性分级策略和管理要求明确数据传输安全策略和操作规程，传输敏感信息应采取加密等安全措施。
d) 针对需进行加密处理的传输业务场景和数据，应部署相应的加密措施，如采用可确保安全的加密算法或传输通道（TLS/SSL 等方式）。
e) 应对数据传输安全策略和操作规程的变更进行审核和监控，包括对密钥使用、传输通道及接口安全配置、密码算法选择、传输协议升级等技术保护措施的审批及监控。

9.5.4 数据销毁安全

a) 应建立数据销毁策略和管理制度，明确销毁对象和流程；并建立数据销毁审批机制，设置销毁相关监督角色，监督操作过程。
b) 能够提供手段协助清除数据因不同设备间共享、业务终止、自然灾害、合同终止等遗留数据，对日志的留存期限应符合国家有关规定。
c) 应提供手段清除数据的所有副本。
d) 数据销毁后应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配前得到完全清除，不可恢复，并做好效果验证。

9.6 OTA 安全

9.6.1 OTA 传输通道安全

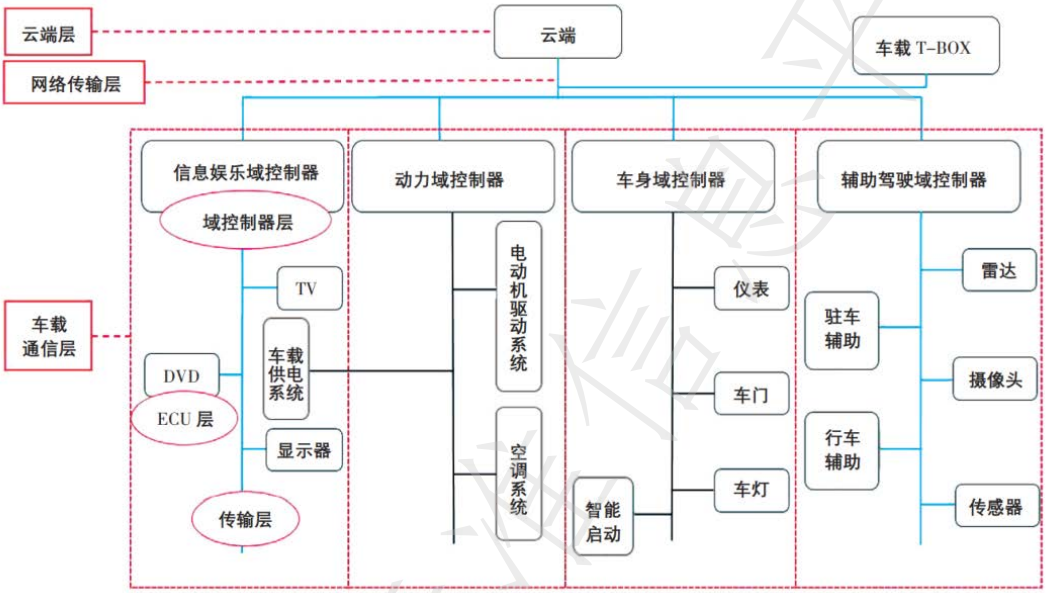
a) 车载终端与 OTA 软件升级服务平台的传输通道应采用 SSL、TLS 等加密方式传输数据。
b) 对于交互过程中敏感数据，例如车载终端设备标识、版本信息等，必须加密保护。
c) OTA 升级在建立传输通道时必须身份认证和授权。

9.6.2 OTA 固件真实性完整性安全

a) 对固件必须采用数字签名技术，至少使用 SHA512 强度级别的哈希算法。
b) 车载终端对固件进行验签，只有验签成功才能升级。

附 录 A

（资料性）
车载终端设备典型逻辑图



附 录 B

（规范性）
V5 接口的安全过程

B.1 概述

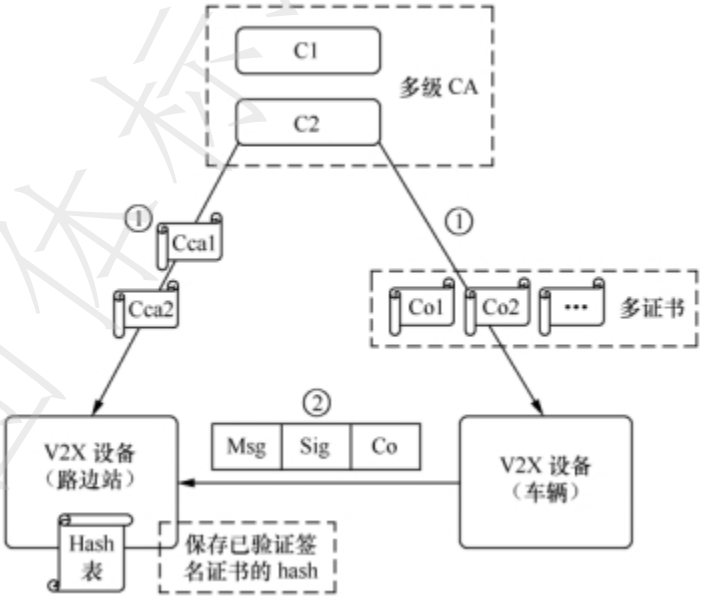
在V2X业务中，V2X设备间通过V5接口交互，安全通信由应用层处理。V2X设备包括V2X车辆 (OBU)、V2X路边单元(RSU)等。通过V5接口提供的通信完整性保护架构如图B.1所示，典型的安全过程如下：

证书管理系统向V2X设备颁发其用于签发消息的公钥证书(安全消息证书)，并以安全的方式向接收消息的V2X设备提供CA公钥证书(以V2X车辆和V2X路边单元通信为例，如图B.1中①所示，C1/C2向V2X车辆下发Co1、Co2、...，向V2X 路边单元下发Cca1、Cca2)。推荐证书管理系统向V2X车辆下发多个公钥证书，V2X车辆每次从这些证书中随机选取一个使用，以保证用户隐私。

V2X设备利用与颁发给它的公钥证书相对应的私钥对消息进行数字签名，将签名消息连同公钥证 书或证书链一同播发出去(如图B.1中②所示，上述消息由需要传递的内容、对内容的签名以及所使用的公钥证书/证书链构成)。此处，接收方的V2X设备可将颁发公钥证书 (Co)的CA证书 (Cca2) 设置为可信证书，接收方的V2X设备利用上述CA证书验证发送方的公钥证书，这样V5接口消息中可以不携带完整证书链，从而节省了空口传输资源。

作为接收方的V2X设备首先利用CA公钥证书验证消息中携带的公钥证书或证书链，然后利用公 钥证书中的公钥验证签名以检查消息的完整性。可选的，接收方V2X设备成功验证对端的公钥证书(Co)后，可将该证书的 hash 值保存在本地，后续可以通过验证证书hash的方式验证该证书，从而减少证书验证所需的密码学操作。

V2X路侧设备到V2X车辆间的通信、V2X车辆到V2X车辆间的通信与上述过程类似。



图B.1 V5 接口安全流程(以V2X 车辆到V2X 路边单元的通信为例)

B.2 安全基本元素说明

安全基本元素说明参见YD/T 3594—2019的6.2。

B.3 安全类数据结构总体要求

在通过PC5接口进行安全类数据数据通信时，其安全的数据结构应统一，其内容应至少包含表B.1信息。具体参见YD/T 3594—2019的6.3。

表B.1 PC5 接口传输的 V5 消息格式

信息	信息版本
	数据类型
	信息内容

B.4 公钥证书格式

B.4.1 消息证书

a) 证书结构

V2X设备设备证书结构的定义应满足GB/T 37376—2019的相关要求。

b) 证书版本

证书的版本号Version的值应设为2，应满足GB/T 37376—2019的相关要求。

c) 签名者信息

签名者信息定义为Issuerld类型，结构应满足GB/T 37376—2019的相关要求。

d) 主题信息

主题信息定义为SubjectInfo类型，结构应满足GB/T 37376—2019的相关要求。

e) 主题属性

主题属性定义为SubjectAttribute 类型，结构应满足GB/T 37376—2019的相关要求。

f) 有效性限定

证书有效性的相关限制定义为ValidityRestriction类型，其中应当至少包括一个time_start_and_end类型，结构应满足GB/T 37376—2019的相关要求。

g) 证书签名

基于公钥密码算法的签名由一个容器封装，定义为Signature类型，结构应满足GB/T 37376—2019的相关要求。

B.4.2 CA证书

CA证书的格式应符合GM/T0015标准要求，应满足GB/T 37376—2019的相关要求。

B.4.3 证书撤销列表

证书撤销列表的格式应满足GB/T 37376—2019的相关要求。

B.5 消息签名流程

B.5.1 概述

签名算法用于确认发送者发送信息的完整性及不可否认性，签名算法应用于且不仅限于以下场景：

a) 证书链验证；

b) 证书系统的策略配置下发；

c) 证书系统颁发的证书撤销列表的下发；

d) 证书请求的生成及验证；

e) V2X 设备之间数据交互。

B.5.2 签名数据结构要求

签名数据应遵循YD/T 3594—2019 6.2的数据结构，其中数据类型应为签名数据类型，信息内容应至少包含见表B.2的信息。具体参见YD/T 3594—2019的6.5.2。

表B.2 签名数据的内容

签名数据	待签名数据	密码杂凑算法描述符
		待签名数据类型

		待签名数据有效时间
		待签名数据值
	签名者信息	
	签名数据结果	签名算法描述符
		签名算法数据存储类型
		签名算法结果值

B.5.3 签名及验签条件限定

签名及验签计算方法应遵循相应签名算法的国际标准，椭圆曲线的参数选择中，应至少支持NIST P-256, brainpoolP256rl及 SM2 三种。

密码杂凑算法应至少支持 SHA256 及 SM3 两种算法。

数据应包含一个被签名的数据区，该区域数据不可更改，任何需要确认且不可更改的数据均应在该区域中。

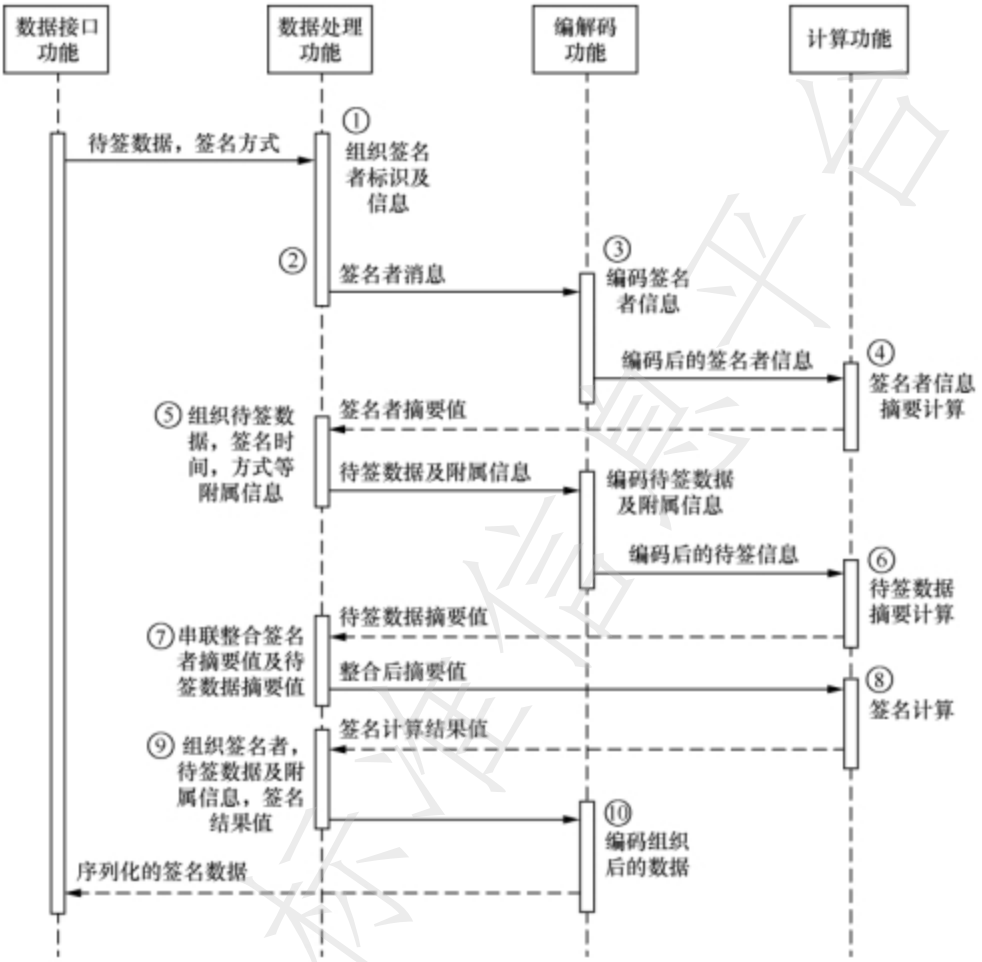
数据应包含一个签名者的识别信息，对于签名消息来说，其签名者信息为对应签名证书的密码杂凑值或对应的签名证书本身，对应证书来说，其签名者信息为对应颁发者证书密码杂凑值或自签标识，对于证书请求来说，其签名者信息为自签标识或者对应的准入证书。

在计算过程中，签名信息的入参数据为待签名数据编码的密码杂凑值与签名者证书编码的密码杂凑值的合并值，其中，如果签名信息为自签的准入证书请求等自签标识，其签名者信息为空，但是其摘要值仍需计算。在签名验签计算过程中，签名算法所使用的密码杂凑算法应满足YD/T 3594—2019附录A的相关要求一致。

在基于 SM2 参数的椭圆曲线算法中，其签名算法应遵循 SM2 签名算法规范，SM2 签名用户可辨别表示应满足YD/T 3594—2019附录A的相关要求。

B.5.4 签名计算流程

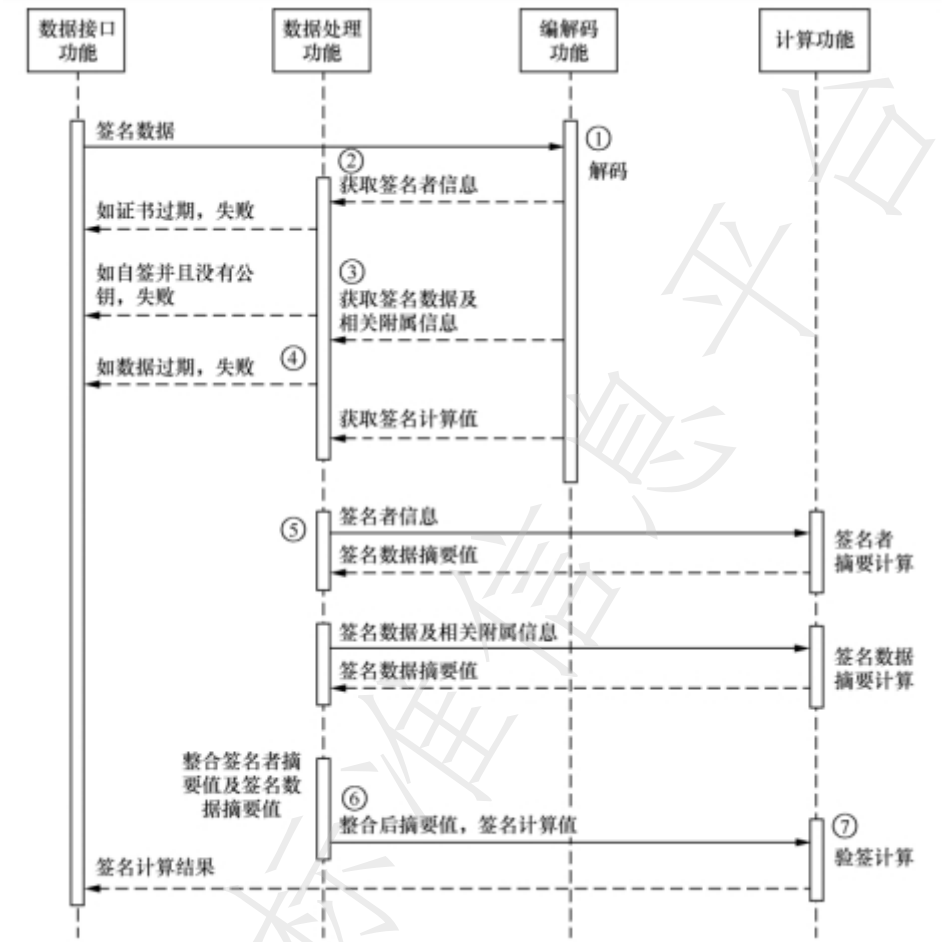
签名计算流程如图B.2所示。具体流程参见YD/T 3594—2019的6.5.4。



图B.2 签名计算流程

B.5.5 验签计算流程

验签计算流程如图B.3所示。具体流程参见YD/T 3594—2019的6.5.5。



图B.3 验签计算流程

B.6 加密消息流程

B.6.1 概述

加密算法用于通信双方实现密文通信，实现信息的机密性，当通信双方需要进行密文通信、以保证信息的机密性时，例如加密算法用于车与车之间应不允许被窃听的双向通信。

B.6.2 加密数据结构要求

加密数据应遵循YD/T 3594—2019 6.2的数据结构，其中数据类型应为加密数据类型，信息内容应至少包含见表B.3的信息。对称密钥数据要求见表B.4。非对称密钥数据要求见表B.5。具体参见YD/T 3594—2019的6.6.2。

表B.3 加密数据

加密数据	对称加密算法标识	
	加密密文数据	原始明文数据长度
		原始明文类型
		原始明文数据
	加密者	加密者类型

		密钥数据值

表B.4 对称加密密钥

对称加密密钥	对称密钥类型
	对称密钥数据值

表B.5 非对称加密密钥

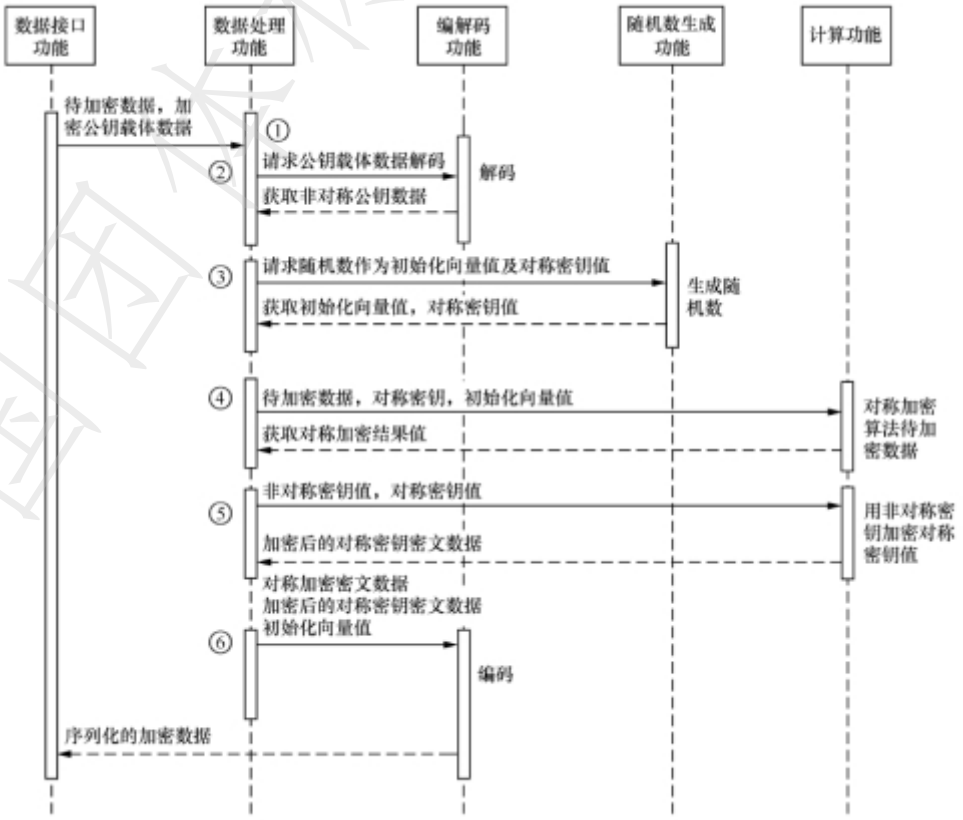
非对称加密密钥	非对称密钥算法	
	非对称密钥载体	非对称密钥载体类型
		非对称密钥载体数据
	非对称加密密钥密文数据	

B.6.3 加密解密条件限定

在使用对称加密算法时，其对称加密算法应至少支持AES128-CCM，SM4-CBC。在使用非对称加密算法时，其非对称加密算法应至少支持 ECIES 、SM2 ，其中ECIES 要求至少支持NIST P-256、brainpoolP256rl两种曲线参数。加密模式应至少包含随机加密模式、协商加密模式两种。加密过程中椭圆曲线上的加密点均应随机生成。对称加密的初始化向量值应每次均随机生成。

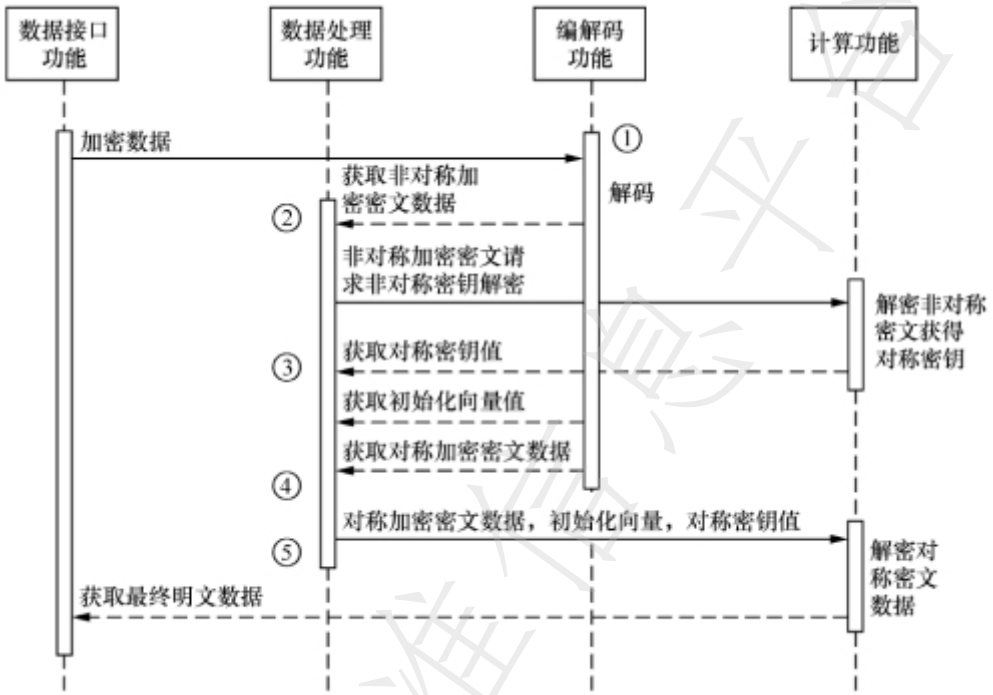
B.6.4 随机加密计算流程

随机加密应由对称加密和非对称加密组合而成，非对称加密应加密对称加密的密钥，而数据则由对称密钥加密。加密流程如图B.4所示。具体流程参见YD/T 3594—2019的6.6.4。



图B.4 随机加密流程

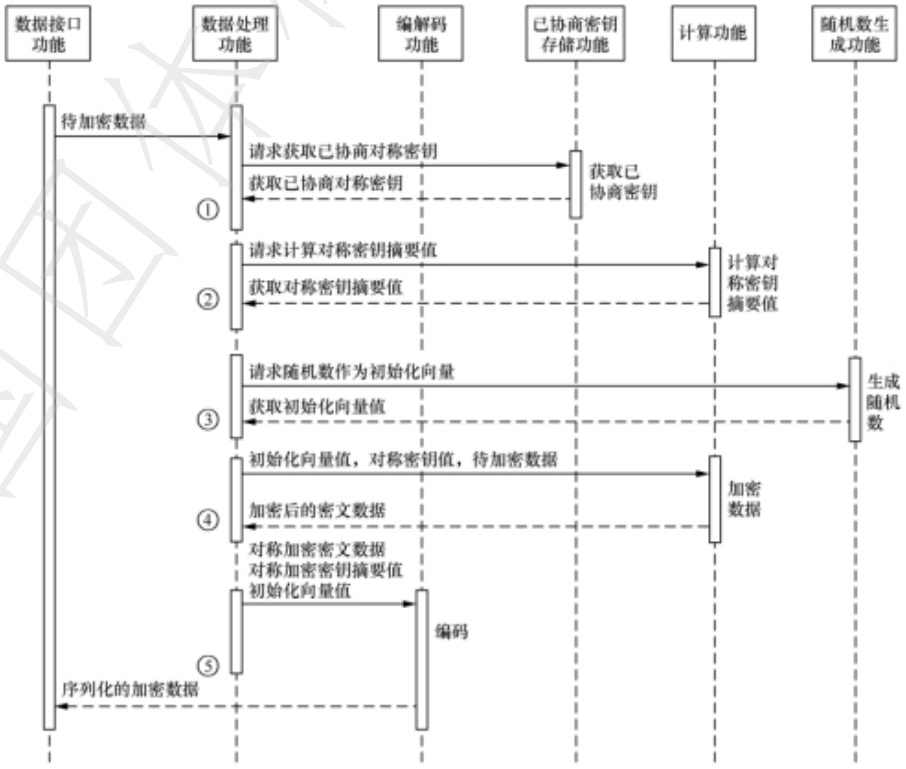
解密流程如图B.5所示。具体流程参见YD/T 3594—2019的6.6.4。



图B.5 随机解密流程

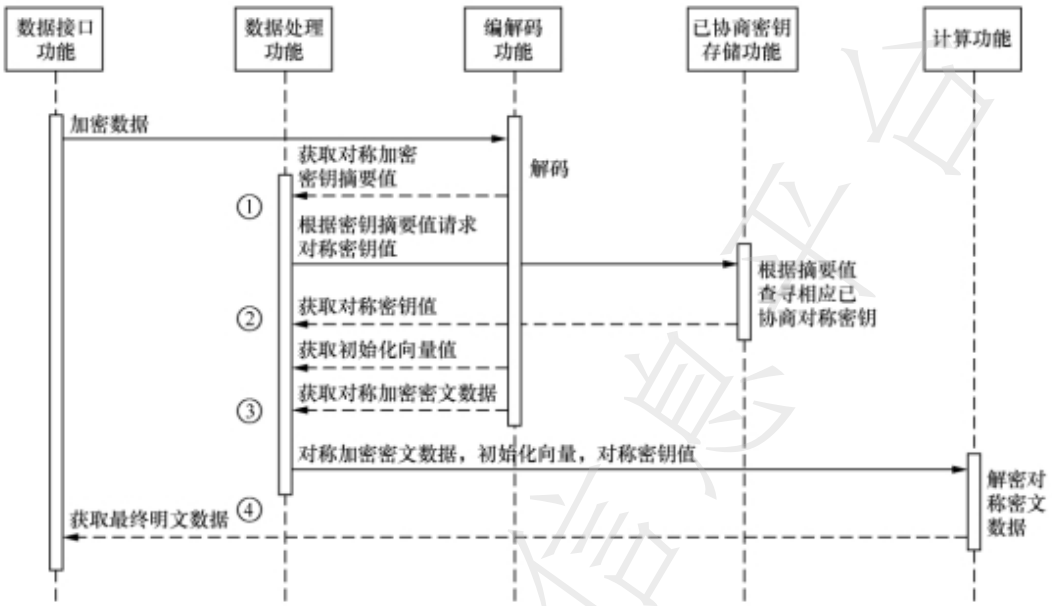
B.6.5 协商加密计算流程

协商加密流程如图B.6所示。具体流程参见YD/T 3594—2019的6.6.5。



图B.6 协商加密流程

协商解密流程如图B.7所示。具体流程参见YD/T 3594—2019的6.6.5。



图B.7 协商解密流程

B.7 密钥协商

B.7.1 密钥协商综述

密钥协商用于通信者A、B双方共同建立会话密钥，密钥协商应满足如下要求：

a) 密钥协商应与协商加密流程同时存在。
b) 协商密钥应存在时间验证机制保障协商密钥定期更换。
c) 通信双方应在协商后保存两个以上协商密钥，保证通信的连续性。
d) 密钥协商的启动条件应满足如下条件，连接初始化或者可用密钥数量少于 2 个。
e) 密钥协商的过程应满足时间条件，超时或过期的协商过程均认为是失败的协商过程。
f) 密钥协商的数据应以密文形式传输，同时密文数据应进行签名计算确定发起者可信。

B.7.2 密钥协商数据结构

密钥协商数据应使用密文数据进行传输，在没有合规的协商密钥时其使用的加密计算流程应使用随机加密计算流程，在存在合规的协商密钥时其使用的加密计算流程应使用协商加密计算流程。所使用数据结构应为加密解密数据结构，其具体数据内容应包含在加密的信息中，标明其明文数据类型为密钥协商数据，其密钥协商数据应至少包含表B.6的内容。具体参见YD/T 3594—2019的6.7.2。

表B.6 密钥协商

密钥协商	协商识别号
	协商报文类型
	协商报文数据

B.7.3 密钥协商计算流程

密钥协商计算流程可参考YD/T 3594—2019的附录E。