ICS 43.040.10

T

宁波市汽车零部件产业协会团体标准

T/NBQLX 001-2021

智能网联汽车终端和零部件信息安全通用技术要求

General Technical Requirements For Information Security Of Intelligent Networked Automobile Terminals And Parts

2021-12-23 发布　　2021-12-23 实施

宁波市汽车零部件产业协会　发布

目　次

前　言

本标准按照 GB/T 1.1-2020 给出的规则起草。

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这些专利的责任。

本标准由宁波市汽车零部件产业协会提出并归口。

本标准主要起草单位：宁波赛宝信息产业技术研究院有限公司、工业和信息化部电子第五研究所、吉利汽车研究院（宁波）有限公司、宁波艾思科汽车音响通讯有限公司、宁波华德汽车零部件有限公司、宁波帅特龙集团有限公司、威睿电动汽车技术（宁波）有限公司、宁波均胜群英智能技术有限公司、宁波均联智行科技股份有限公司。

本标准主要起草人：接军、王洪涛、金桂芳、李乐言、王律、冷振华、胡玉格、方桢峰、胡达锋、励春林、王立献、娄本杰、刘刚、凌平、陈翔等。

智能网联汽车终端和零部件信息安全通用技术要求

1 范围

本标准规定了智能网联汽车车载终端和零部件的信息安全技术要求，包括硬件安全、操作系统安全、软件安全、数据安全、通信安全和个人信息安全。

本标准适用于智能网联汽车车载终端和零部件的研制、生产、测试、评估与认证，包括不限于 T-BOX、IVI、车载网关、车载防火墙等终端和零部件。

2 规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 25069-2010 信息安全技术 术语

GB/T 18336-2015 信息技术 安全技术 信息技术安全性评估准则

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 40855-2021 电动汽车远程服务与管理系统信息安全技术要求及试验方法

GB/T 40856-2021 车载信息交互系统信息安全技术要求及试验方法

GB/T 40857-2021 汽车网关信息安全技术要求及试验方法

GB/T 40861-2021 汽车信息安全通用技术要求

YD/T 3746-2020 车联网信息服务 用户个人信息保护要求

YD/T 3750-2020 车联网无线通信安全技术指南

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 3957-2021 基于LTE的车联网无线通信技术 安全证书管理系统技术要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

智能网联汽车 intelligent connected vehicles

智能网联汽车是指搭载先进的车载传感器、控制器、执行器等装置，并融合现代通信与网络技术，实现车与 X（人、车、路、云端等）智能信息交换、共享，具备复杂环境感知、智能决策、协同控制等功能，可以实现安全、高效、舒适、节能行驶，并最终可实现替代人来操作的新一代汽车。智能网联汽车通常也被称为智能汽车、自动驾驶汽车等。

3.2

数字签名 digital signature

数字签名是只有信息的发送者才能产生的别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。保证数据来源的真实性和和完整性，防止数据被第三方

伪造，保护发送者。

3.3

端口 port

设备与外界通信交流的出口，本文特指 TCP/IP 协议中的端口，是逻辑意义上的端口。

3.4

外围接口 peripheral interface

分为有线外围接口和无线外围接口。有线外围接口包括USB接口、SD卡接口等，无线外围接口包括蓝牙接口、WLAN接口等。

3.5

车载终端 on-board terminal

安装在汽车上，采集及保存整车及系统部件的关键状态参数并发送到平台的装置或系统。

[来源：GB/T 32960.1-2016,3.4]

4 缩略语

T-BOX	车联网盒子	Telematics BOX
IVI	车载信息娱乐系统	In-Vehicle Infotainment
PCB	印制电路板	Printed Circuit Board
BGA	焊球阵列封装	Ball Grid Array
LGA	栅格阵列封装	Land Grid Array
CNNVD	中国国家信息安全漏洞库	China National Vulnerability Database of Information Security
CNVD	国家信息安全漏洞共享平台	China National Vulnerability Database

5 技术要求

5.1 硬件安全

5.1.1 硬件标识安全

硬件标识安全要求如下：

a)硬件整机应具备唯一性标识；

b)硬件PCB不应存在功能丝印标识，比如用于标注芯片、调试接口、管脚功能等的可读丝印。

5.1.2 硬件接口安全

在生产、调试或者维护时需要使用调试接口，调试接口应禁用或设置安全访问控制。

5.1.3 芯片安全

终端和零部件所使用的芯片的芯片安全要求如下：

a)应减少暴露管脚，如采用BGA/LGA等封装芯片；

b)应具备足够的安全机制保证密钥的产生、分发、存储和销毁过程的安全性；

c)关键加密算法实现应具备抵抗物理层攻击的能力，防止根密钥被破解，包括密码分析攻击、侧信

道攻击、故障注入攻击等。

5.2 操作系统安全

5.2.1 安全启动

应具备安全启动的功能，可通过可信根实体对安全启动所使用的可信根进行保护。

5.2.2 端口与服务安全

系统提供的端口与服务安全要求如下：

a)基于端口开放最小化原则，默认关闭不是系统业务所必需的其他端口；

b)操作系统按照模块最小化裁剪仅保留必须的模块。

5.2.3 漏洞与缺陷管理安全

漏洞与缺陷管理安全要求如下：

a)系统及预置应用软件应保证不包含有 CNVD 与 CNNVD 6 个月前公布的高危及以上的漏洞；

b)预装软件、补丁包/升级包应不包含恶意程序。

注：处置包括消除漏洞、制定减缓措施等方式。

5.2.4 系统权限控制

系统权限控制要求如下：

a)对于支持多个用户账号的系统，要对账号进行分级分权，不得越权操作；

b)系统应对远程接入控制的请求进行身份验证；

c)系统不应预留任何未公开帐号，所有帐号应在操作系统管理范围内；

d)禁止用户修改或者卸载系统预装的核心应用。

5.2.5 系统与固件升级安全

系统与固件升级安全要求如下：

a)应支持固件和系统远程升级；

b)应对升级包的来源和完整性进行校验，包括验证升级包的哈希值、文件大小、版本号和签名；

c)当发生更新失败时，设备能回退到原来的版本，可以正常启动；

d)应提供系统升级的日志记录功能，确保异常升级时可以溯源，日志存储不少于 6 个月；

e)升级包文件应做防篡改或其他合适的加密处理；

f)升级包应采用加密通道传输。

5.3 软件安全

5.3.1 预置应用软件的安全

如具备预置应用软件，预置应用软件安全应满足如下要求：

a)预置的应用软件要进行加固处理，防止反编译、二次打包，反调试等；

b)预置的应用软件权限遵循最小化原则；

c)预置的应用软件不应存在后门等隐藏接口。

5.3.2 第三方应用软件的安装安全

如支持第三方应用软件安装，第三方应用软件的安装安全应满足如下要求：

a)禁止安装未经授权签名的第三方应用；

b)防止运行外接设备里的可疑脚本或者可执行程序；

c)需校验该应用软件的完整性以及数字签名，数字签名算法采用安全的算法。

5.3.3 应用软件的更新安全

如支持应用软件的更新，应满足如下要求：

a)预置应用软件进行更新时，应对应用软件更新包进行版本号、哈希值、签名和文件大小校验；

b)进行预置应用软件更新时，宜对应用软件更新包进行加密，防止应用更新包被非法获取，导致信息泄露。

5.4 数据安全

根据数据的生命周期，数据安全分为数据采集、数据传输、数据存储和使用、数据删除四个方面。

5.4.1 数据采集安全

数据采集安全要求如下：

a)应在用户已知确认下，才能收集用户的数据，防止未向用户明示且未经用户同意，收集用户数据的行为；

b)防范未经授权的下载、篡改、删除等操作，只有被授权的应用程序才能读取或修改数据，未经授权的应用程序不能对数据进行操作。

5.4.2 数据传输安全

数据传输安全要求如下：

a)针对传输数据被恶意篡改的现象，需要对重要数据的传输通道进行加密保护，保证传输过程中数据的完整性；

b)支持传输过程中的身份鉴别和认证。

5.4.3 数据存储和使用安全

数据存储和使用安全要求如下：

a)对重要数据进行加密存储，不能以硬编码的形式存储在终端和和零部件中；

b)安全重要参数在存储以及使用过程中，应只允许被授权的应用以授权方式读取和修改；

c)应支持数据可用性保障，支持数据备份和恢复的能力。

5.4.4 数据删除安全

数据删除安全要求如下：

a)在恢复出厂设置时应删除运行的数据和配置文件；

b)在返厂维修时，支持数据被彻底删除的功能，以保证被删除的数据不可再恢复，防止残留的数据信息被泄露或非法获取。

5.5 通信安全

5.5.1 通信完整性

应采用杂凑密码算法（如 SM3）和数字签名算法（如 SM2）的检验技术和密码技术保证重要数据在传输和存储过程中的完整性，包括鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

5.5.2 通信机密性

应采用对称密码算法（如 SM4）和数字信封分发对称密钥的方式的检验技术和密码技术保证重要数据在传输和存储过程中的保密性，包括鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

5.5.3 抗数据重放

应能够采用时间戳或缓存队列等方式鉴别数据的新鲜性，避免历史数据的重放攻击，应能够鉴别历史数据的非法修改，避免数据的修改重放攻击。

5.5.4 行为抵赖

数据传输应具备抵赖性，发送方用自己的私钥对传输的数据进行签名，接收方使用发送方的公钥对签名数据验签，防止发送方对其行为进行抵赖。

5.6 个人信息安全

终端和零部件涉及智能网联汽车个人信息的需符合 GB/T 35273—2020 的要求，智能网联汽车个人信息分类见附录 A。

附 录 A

（规范性附录）

智能网联汽车个人信息分类

用户个人信息是指信息服务如数据采集传输和使用销毁等过程中与用户密切相关的数据信息，这些数据信息能够一定程度上识别用户个人身份或反映处用户个人活动情况。信息服务用户个人信息细分为用户身份证明类信息、信息服务用户数据和服务内容信息、用户服务相关信息三大类。

用户身份证明类信息：是指信息服务活动过程中与用户自然人身份和标识信息、用户虚拟身份和鉴权信息密切相关的用户个人信息。

用户数据和服务内容信息：主要信息服务过程中用户服务内容信息和用户资料信息。其中，用户服务内容信息包括驾驶及行车安全服务信息、生活服务信息、交通出行管理服务信息、交通出行管理服务信息、涉车服务信息、行业营运服务信息；用户资料信息涉及联系人信息、用户私有资料数据和信息服务内容衍生信息等。

用户服务相关信息：指信息服务过程中用户服务使用信息、用户车辆基本标识信息和用户设备、系统和平台信息。

表 A.1 个人信息举例

用户个人信息类别		用户个人信息范围	用户个人信息示例
A:用户身份证明类信息	A1:用户自然人身份和标识信息	A1-1:用户基本资料	姓名、证件类型及号码、年龄、性别、职业、工作单位、地址、宗教信仰、民族、国籍、电话号码等
		A1-2:用户身份证明	身份证、军官证、护照、机动车驾驶证、社保卡等证件影印件
		A1-3:用户生理标识	指纹、声纹、虹膜、脸谱等
	A2：用户虚拟身份和鉴权信息	A2-1:普通信息服务身份标识和鉴权信息	电话号码、账号、邮箱地址、用户个人数字证书以及服务涉及的密码、口令、密码保护答案、解锁图案等
		A2-2：交易类信息服务身份标识和鉴权信息	各类交易账号和相应的密码、密码保护答案、解锁图案、系统或平台中登录的个人银行账号、交易验证码、动态口令、交易信息等
B:信息服务内容类用户数据信息	B1:用户服务内容信息	B1-1:驾驶及行车安全服务类信息	智能辅助驾驶相关服务场景下的车辆驾驶行为、行经路线等信息；在车辆防碰撞（如碰撞预警、紧急刹车预警、变道预警、车辆失控预警、异常车辆预警等）、车车编队辅助和防撞人或物等服务中相关的用户个人信息
		B1-2：生活服务信息	生活服务相关的内容信息，如个人数据文件、邮件服务、广播服务、网页浏览、购物、在线音乐和视频服务、天气预报及推送、社交服务、移动办公服务等用户个人信息

用户个人信息类别		用户个人信息范围	用户个人信息示例
		B1-3：交通出行管理服务信息	在交通动态信息通知服务（如信号灯信息推送、红绿灯车速引导、闯红灯预警等信息）中相关的个人信息； 在浮动车交通管理（如车辆信息动态交换采集、违法信息抓拍上报、停车诱导和管理、交通流量疏导、交通应急信息发布等）服务中相关的用户个人信息
		B1-4：涉车服务信息	在涉车服务（如 UBI 保险和交易、分时租赁和约车拼车、车辆检修保养救援）等相关的用户个人信息
		B1-5：行业营运服务信息	在行业营运服务中相关的内容信息（如公交、处在、物流、换位、港口、景区等运营车辆管理），如与车况和位置信息上报、远程控制、越界和超速预警、特定区域特定路线特定行业下自动驾驶等相关的用户个人信息
	B2：用户资料信息	B2-1：联系人信息	通信录、好友列表等用户资料数据； 车内蓝牙配对拷贝的联系人列表
		B2-2：用户私有资料数据	用户云存储、终端、SD 卡等存储的用户文字、多媒体等资料数据信息
		B2-3：信息服务内容衍生信息	基于定位及导航服务内容分析获取的车辆活动轨迹、精准定位信息、个人生活习惯、健康状况等资料信息
C：用户服务相关信息	C1：用户服务使用信息	C1-1：业务订购、订阅关系	业务订购信息、业务注册时间、修改、注销状况信息等
		C1-2：服务记录	信息服务平台、智能网联汽车及智能终端中存储或缓存的直接或间接产生的用户操作记录，如信息服务中涉及的照片、音频、视频、通话记录等；浏览的新闻或购物浏览器访问的网址列表；娱乐软件记录、汽车远程操控指令记录、语音服务的系统备份信息、网页购物记录等
		C1-3：日志	反映用户操作记录的如日志信息、日志文件等
		C1-4：交易服务信息	交易信息、消费记录、流水记录等
	C2：用户车辆基	C2-1：车辆基本资料	车辆类型、车辆品牌、车辆型号、

用户个人信息类别		用户个人信息范围	用户个人信息示例
	本标识信息		车辆底盘型号、发动机号、燃油种类、车牌号、发动机号、车辆识别代码（VIN 码）等
	C3：用户设备、系统和平台信息	C3-1:设备、系统或平台信息	硬件型号、唯一设备识别码 IMEI、设备/系统/平台 MAC 地址、SIM 卡 IMSI 信息等