ICS 43.040.10

T

宁波市汽车零部件产业协会团体标准

T/NBQLX 002-2021

智能网联汽车终端和零部件信息安全通用测试规范

General Test Specification For Information Security Of Intelligent Connected Vehicle 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、马广义、许海霞、俞建能、李胜旺、胡达锋、江华侨、陈存定、刘凤丹、顾广东、凌平、陈翔等。

智能网联汽车终端和零部件信息安全通用测试规范

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 测试规范

5.1 硬件安全测试

5.1.1 硬件标识安全测试

测试步骤：

步骤一：终端或零部件处于正常工作状态。

步骤二：通过拆机检查，检查如下内容：

a)硬件整机是否具备唯一性标识；

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

步骤三：结果若符合 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》5.1.1 要求，判定为符合，其他情况判定为不符合。

5.1.2 硬件接口安全测试

测试步骤：

步骤一：终端或零部件处于正常工作状态。

步骤二：通过拆机检查，检查如下内容：

调试接口是否禁用或设置安全访问控制。

步骤三：结果若符合 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》5.1.2 要求，判定为符合，其他情况判定为不符合。

5.1.3 芯片安全测试

测试步骤：

步骤一：终端或零部件处于正常工作状态。

步骤二：通过芯片侧信道、安全扫描等测试工具，检查如下内容：

a)是否暴露管脚，如采用BGA/LGA等封装芯片；

b)是否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。

步骤三：结果若符合 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》5.1.3 要求，判定为符合，其他情况判定为不符合。

5.2 操作系统安全测试

5.2.1 安全启动测试

测试步骤：

步骤一：终端或零部件处于正常工作状态。

步骤二：通过刷写 bootloader 等分析手段检查如下内容：

检查是否具备安全启动的功能。

步骤三：结果若符合 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》5.2.1 要求，判定为符合，其他情况判定为不符合。

5.2.2 端口与服务安全测试

测试步骤：

步骤一：终端或零部件处于正常工作状态。

步骤二：通过数据包嗅探、修改和重放等分析手段检查如下内容：

a)基于端口开放最小化原则，是否默认关闭不是系统业务所必需的其他端口；

b)操作系统是否按照模块最小化裁剪仅保留必须的模块。

步骤三：结果若符合 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》5.2.2 要求，判定为符合，其他情况判定为不符合。

5.2.3 漏洞与缺陷管理安全测试

测试步骤：

步骤一：终端或零部件处于正常工作状态。

步骤二：通过漏洞扫描等分析手段检查如下内容：

a)系统是否保证不包含有 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/升级包是否包含恶意程序。

步骤三：结果若符合 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》5.2.3 要求，判定为符合，其他情况判定为不符合。

5.2.4 系统权限控制测试

测试步骤：

步骤一：终端或零部件处于正常工作状态。

步骤二：通过系统权限功能验证检查如下内容：

a)对于支持多个用户账号的系统，是否对账号进行分级分权，是否存在越权操作；

b)系统是否对远程接入控制的请求进行身份验证；

c)系统是否预留任何未公开帐号，所有帐号是否在操作系统管理范围内；

d)是否禁止用户修改或者卸载系统预装的核心应用。

步骤三：结果若符合 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》5.2.4 要求，判定为符合，其他情况判定为不符合。

5.2.5 系统与固件升级安全测试

测试步骤：

步骤一：终端或零部件处于正常工作状态。

步骤二：通过漏洞扫描等分析手段检查如下内容：

a)是否支持固件和系统远程升级；

b)是否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，设备是否能回退到原来的版本，可以正常启动；

d)是否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)升级包文件是否做防篡改或其他合适的加密处理；

f)升级包是否采用加密通道传输。

步骤三：结果若符合 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》5.2.5 要求，判定为符合，其他情况判定为不符合。

5.3 软件安全测试

5.3.1 预置应用软件的安全测试

测试步骤：

步骤一：终端或零部件处于正常工作状态。

步骤二：通过漏洞扫描等分析手段检查如下内容：

a)预置的应用软件是否进行加固处理，防止反编译、二次打包，反调试等；

b)预置的应用软件权限是否遵循最小化原则；

c)预置的应用软件是否存在后门等隐藏接口。

步骤三：结果若符合 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》5.3.1 要求，判定为符合，其他情况判定为不符合。

5.3.2 第三方应用软件的安装安全测试

测试步骤：

步骤一：终端或零部件处于正常工作状态。

步骤二：通过漏洞扫描等分析手段检查如下内容：

a)是否禁止安装未经授权签名的第三方应用 APP；

b)是否支持第三方应用软件安装，是否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。

步骤三：结果若符合 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》5.3.2 要求，判定为符合，其他情况判定为不符合。

5.3.3 应用软件的更新安全测试

测试步骤：

步骤一：终端或零部件处于正常工作状态。

步骤二：通过漏洞扫描等分析手段检查如下内容：

a)预置应用软件进行更新时，是否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，是否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。

步骤三：结果若符合 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》5.3.3 要求，判定为符合，其他情况判定为不符合。

5.4 数据安全测试

5.4.1 数据采集安全测试

测试步骤：

步骤一：终端或零部件处于正常工作状态。

步骤二：通过数据包嗅探、修改和重放等分析手段检查如下内容：

a)是否在用户已知确认下，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)是否防范未经授权的下载、篡改、删除等操作，是否只有被授权的应用程序才能读取或修改数据，是否未经授权的应用程序不能对数据进行操作。

步骤三：结果若符合 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》5.4.1 要求，判定为符合，其他情况判定为不符合。

5.4.2 数据传输安全测试

测试步骤：

步骤一：终端或零部件处于正常工作状态。

步骤二：通过数据包嗅探、修改和重放等分析手段检查如下内容：

a)针对传输数据被恶意篡改的现象，是否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)是否支持传输过程中的身份鉴别和认证。

步骤三：结果若符合 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》5.4.2 要求，判定为符合，其他情况判定为不符合。

5.4.3 数据存储和使用安全测试

测试步骤：

步骤一：终端或零部件处于正常工作状态。

步骤二：通过数据包嗅探、修改和重放等分析手段检查如下内容：

a)识别用户敏感数据，是否对敏感数据进行加密存储，是否以硬编码的形式存储在终端和和零部件中；

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

c)是否支持数据可用性保障，支持数据备份和恢复的能力。

步骤三：结果若符合 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》5.4.3 要求，判定为符合，其他情况判定为不符合。

5.4.4 数据删除安全测试

测试步骤：

步骤一：终端或零部件处于正常工作状态。

步骤二：通过数据包嗅探、修改和重放等分析手段检查如下内容：

a)在恢复出厂设置时是否删除运行的数据和配置文件；

b)在返厂维修时，是否支持数据被彻底删除的功能，是否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。

步骤三：结果若符合 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》5.4.4 要求，判定为符合，其他情况判定为不符合。

5.5 通信安全测试

5.5.1 通信完整性测试

测试步骤：

步骤一：终端或零部件处于正常工作状态。

步骤二：通过数据包嗅探、修改和重放等分析手段检查，是否采用杂凑密码算法（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。

步骤三：结果若符合 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》5.5.1 要求，判定为符合，其他情况判定为不符合。

5.5.2 通信机密性测试

测试步骤：

步骤一：终端或零部件处于正常工作状态。

步骤二：通过数据包嗅探、修改和重放等分析手段检查，是否采用对称密码算法（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。

步骤三：结果若符合 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》5.5.2 要求，判定为符合，其他情况判定为不符合。

5.5.3 抗数据重放测试

测试步骤：

步骤一：终端或零部件处于正常工作状态。

步骤二：通过数据包嗅探、修改和重放等分析手段检查，是否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。

步骤三：结果若符合 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》5.5.3 要求，判定为符合，其他情况判定为不符合。

5.5.4 行为抵赖测试

测试步骤：

步骤一：终端或零部件处于正常工作状态。

步骤二：通过数据包嗅探、修改和重放等分析手段检查，数据传输是否具备抵赖性，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。

步骤三：结果若符合 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》5.5.4 要求，判定为符合，其他情况判定为不符合。

5.6 个人信息安全测试

测试步骤：

步骤一：终端或零部件处于正常工作状态。

步骤二：通过个人信息保护合规审查等分析手段检查，终端和零部件涉及智能网联汽车个人信息的是否符合GB/T 35273—2020的要求。

步骤三：结果若符合 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》5.6 要求，判定为符合，其他情况判定为不符合。