ICS 43.020

CCS T 40

团　　体　　标　　准

T/GHDQ 93-2022

移动终端控车应用软件信息安全技术要求

Information Security Technical Requirements for Mobile Terminal Vehicle Control Application Software

2022-10-23 发布　　2022-10-24 实施

吉林省汽车电子协会　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。

本文件由中国第一汽车集团有限公司智能网联开发院提出。

本文件由吉林省汽车电子协会归口。

本文件由吉林省汽车电子协会组织实施。

本文件主要起草单位：中国第一汽车集团有限公司智能网联开发院。

本文件主要起草人：陈明、高长胜、李木犀、吴淼、刘毅、高铭霞、边泽宇、邵馨蕊、胡闯、于欢、陈后立、杨雪珠。

本文件参与起草单位：中汽创智科技有限公司、吉林大学汽车仿真与控制国家重点实验室、吉林大学通信工程学院、华晨宝马汽车有限公司、东风汽车集团有限公司技术中心、一汽解放汽车有限公司、一汽奔腾轿车有限公司、中国汽车技术研究中心有限公司、武汉路特斯科技有限公司、富赛汽车电子有限公司、重庆长安汽车股份有限公司。

本文件参与起草人：徐敏杰、李杰、高金武、王思涵、孙伟、梁亚丽、王晓光、李宝田、刘建鑫、赵岩、汪向阳、罗薇。

本文件审查人：周时莹（中国第一汽车集团有限公司智能网联开发院）、卢放（岚图汽车科技有限公司）、何文（重庆长安汽车股份有限公司）、夏国强（中国汽车工程研究院股份有限公司）、孔晓霜(中国第一汽车集团有限公司创新技术研究院)。

本文件为首次发布。

引　言

近年来，我国智能网联汽车产业高速发展，便捷化、实用化功能越来越受客户欢迎。智能网联汽车越来越多的业务场景采用移动终端应用软件来进行控制和实现，比如数字钥匙、远程控车等。越来越多的应用场景的涌现，给部署在移动终端上的应用软件带来了新的挑战和安全问题。针对移动终端控车应用软件进行专门的信息安全技术要求变越来越迫切。

因此，有必要编制一个基础性标准对移动终端控车应用软件的信息安全技术进行规范化要求，统一设计要点，形成平台化技术要求，以保证移动终端控车应用软件的安全性和一致性。

为了确保标准的规范化和普适性，本规范在基础安全、应用安全、数据安全、通信安全等安全技术要点进行要求和规范。以形成通用性的技术要求。

移动终端控车应用软件信息安全技术要求

1. 范围

本文件规定了智能网联汽车移动终端控车应用软件信息安全的技术要求。

本文件适用于智能网联汽车移动终端控车应用软件信息安全,指导此类业务的信息安全技术的设计开发 、验证、生产等工作。

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 37729-2019 信息技术 智能移动终端应用软件(APP)技术要求

YD/T 3082-2016 移动智能终端上的个人信息保护技术要求

3. 术语和定义

下列术语和定义适用于本文件。

3.1

应用软件 Application Software; App

针对智能移动终端设备开发的专门解决应用问题的软件。

4. APP 基础安全

4.1. 来源安全

来源安全要求如下:

a) APP只能通过车企官方渠道或车企授权的合法渠道下载安装;

b) APP应进行相应渠道的签名,应进行完整性校验,防止被非法篡改;

c) APP安装、升级时,应对APP安装包或升级包进行签名的验证。

4.2. 代码安全

代码安全要求如下:

a) 应对APP代码进行混淆保护,同时进行安全加固以对抗源代码反编译攻击行为;

b) 应确保APP使用的开源代码及第三方组件代码的安全性及合规性;

c) 确保发布的APP不存在权威渠道已发布的高中危漏洞,并对权威渠道漏洞持续监测并迭代修补;

d) APP应具有防动态调试功能,确保攻击者无法通过动态调试方法获得程序内部运行逻辑;

e) APP应对自身的资源文件进行保护,防止被恶意攻击和调试分析;

f） APP应具有防进程注入功能，防止攻击者通过hook挂钩的方式将恶意进程注入到APP中。

5. APP 应用安全

5.1. 访问控制

访问控制要求如下：

a） 应设置APP访问权限，对参与跨APP调用的组件设置访问权限；
b） 应对授权访问的内容执行访问控制策略，不具备访问权限的应用或用户无法访问该APP；
c） APP访问移动终端的资源应得到用户明确的授权，未授权不允许访问；
d） 用户授权或修改APP权限后，应直接生效，不需要重启系统；
e） 应针对APP访问权限进行管理，使用最小化服务权限进行访问，对系统核心资源的访问，应采用访问控制措施，限制访问；
f） 赋予APP功能和权限时，只赋予完成操作的必备权限和最少功能。

5.2. 身份鉴别

身份鉴别要求如下：

a） 应根据业务需要，提供登录控制，对用户进行身份认证和鉴别；
b） APP登录应在服务端进行验证，不允许在客户端进行验证；
c） 重要功能操作时，应进行二次认证；
d） 同一时间用户只能在一处登录，不允许同一用户在多个移动终端同时登录；
e） 用户设置的口令应具备一定的安全强度，不允许设置弱口令；
f） APP应具备防暴力破解保护功能，10分钟内登录失败次数超过3次锁定该账户半个小时；
g） 用户登录失败提示信息模糊处理，提示信息中不应泄露用户账号注册情况；
h） 用户修改或找回口令，APP应具备验证保护机制。

5.3. 操作安全

操作安全要求如下：

a） APP人机交互接口应确保安全性，防止通过人机交互接口进行注入攻击等行为；
b） 用户输入的错误指令应进行合理的操作提示，避免泄露用户隐私及APP运行环境信息；
c） 用户执行远程控制指令时，应确认用户身份，确保用户具备操作权限。

5.4. 日志安全

日志安全要求如下：

a） APP应记录用户的操作日志不低于60天；
b） APP记录的日志不应向无授权用户或应用进行展示和读取；
c） APP日志记录中不应存在用户隐私数据，必要时进行脱敏和加密处理；
d） APP运行日志、错误日志仅记录用来维护APP运行的信息，不应泄露运行环境及个人信息。

6. APP 数据安全

6.1. 合规性要求

合规性要求如下：

a） APP采集和使用用户的数据前应得到用户的明确授权；
b） 未经用户授权，APP不得以任何理由采集和使用用户数据；
c） APP在采集、使用和传输过程中不得非法截留和保存用户数据；
d） 用户敏感数据在传输和存储过程中需要脱敏、加密处理；
e） 采集和使用用户的信息应遵循合理合法合规的原则，明确告知用户信息收集的方式、使用的目的和范围。

6.2. 数据保护要求

数据保护要求如下：

a） APP传输和保存的用户数据应进行加密保存，敏感数据应存储在安全区域；
b） 用户敏感信息在使用和存储时应脱敏处理；
c） 用户特征数据的使用应在APP端进行，不应传输到云端；
d） APP卸载、删除时应同时删除存储的用户信息。

6.3. 数据备份和恢复

数据备份和恢复要求如下：

a） APP应有数据备份机制，并对备份的数据进行安全保护；
b） APP执行数据恢复时应验证备份数据的完整性；
c） APP异常关闭或退出时，数据应能进行及时备份。

7. APP 通信安全

7.1. 安全通道

安全通道要求如下：

a） APP与后台的通信应采用不低于TLS1.2的安全通道进行；
b） APP与后台通信前应进行身份验证，应采取双向认证方式；
c） 重要远控指令数据在安全通道中传输前应进行应用层加密。

7.2. 通信保持

通信保持要求如下：

a） APP与后台通信过程中，如有电话、语音等通讯时，优先进行即时通讯的接通，并在结束及时通讯后能及时恢复APP与后台的通信；
b） APP与后台通信异常时，应及时提醒用户知晓；
c） APP与后台通信完毕后应及时断开连接，减少资源浪费的同时降低被攻击面。