

T/ITS

中国智能交通产业联盟标准

T/ITS 0068—2017

基于公众电信网的联网汽车信息安全技术 要求

Technology requirements of connected vehicle cybersecurity based on public
telecommunication network

2017-12-10 发布

2018-03-01 实施

中国智能交通产业联盟 发布

目 次

前言 II

引言 III

1 范围 1

2 规范性引用文件 1

3 术语 1

4 缩略语 2

5 汽车联网系统架构 4

6 联网汽车网络架构安全技术要求 5

7 联网通信安全技术要求 7

8 联网数据隐私安全技术要求 13

前 言

《基于公众电信网的联网汽车信息安全技术要求》作为基于公众电信网信息安全方面的纲领性标准，为接入公众电信网络的汽车提供必要的信息安全标准化保障。

本标准依据 GB/T1.1-2009 给出的规则起草。

本标准由中国智能交通产业联盟提出并归口。

本标准起草单位：中国智能交通产业联盟、中国信息通信研究院、奇虎 360 科技有限公司、西安电子科技大学、上海车音智能科技有限公司。

本标准主要起草人：刘健皓、葛雨明、刘家佳、张林、吕欣鸿、杨明坤。

引 言

该标准主要适用于接入公众电信网络的联网汽车，为联网汽车信息安全提供指导性建议供汽车厂商、零部件供应商、信息安全厂商参考。

标准内容主要利用通信安全技术来降低汽车信息安全风险的影响范围，从而达到相对安全的态势。定义了联网汽车数据的类型，针对不同类型数据应用的安全防护手段，保障联网汽车数据隐私安全。同时将动态的监控、检测、响应机制与汽车运营相结合，形成基于公众电信网的网联汽车的动态防护框架，从而能够保障基于公众电信网的汽车安全稳定的运营。

为了保持标准的适应性与可操作性，各使用者在采标过程中，及时将本标准规范的意见及建议函告知编写单位，一遍修订时研用。

地址：北京市朝阳区酒仙桥路6号院2号楼，邮编：100015，邮箱:liujianhao@360.cn

基于公众电信网的联网汽车信息安全技术要求

1 范围

本标准规范了基于公众电信网的联网汽车的信息安全技术要求，在通信安全、数据安全、控制安全方面的信息安全技术进行了规范。

本标准适用于联接公众电信网络的汽车终端安全技术要求。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所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 20271-2006 信息安全技术 信息系统安全通用技术要求

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求

GM/T 0006-2012 密码应用标识规范

GB/T 21054-2007 信息安全技术 公钥基础设施 PKI系统安全等级保护评估准则(1)

GA T387-2002 《计算机信息系统安全等级保护网络技术要求》

MSTL_JGF_04-009 信息安全技术文件加密产品检验规范

MSTL_JGF_04-020 信息安全技术Web过滤防护产品检验规范

MSCTC-GFJ-03 信息技术VPN产品安全检验规范

YD-T 1765-2008 通信安全防护名词术语

GB/T 21053—2007 PKI系统安全等级保护技术要求

YD-T 1699-2007 移动终端信息安全技术要求

YD-T 1621-2007 网络与信息安全服务资质评估准则

MSTL_JGF_04-018信息安全技术日志分析产品检验规范

YD-T 2407-2013 移动智能终端安全能力技术要求

3 术语

下列术语和定义适用于本文件。

3.1

联网汽车 Connected vehicle

指带有接入互联网服务与应用并具有远程控制功能的汽车。

3.2

用户策略 Profile

车联网向用户提供服务所需的数据和应用的集合，需要通过配置文件的及数据的形式存放在云端管理平台，为用户提供定制化的服务。

3.3

静态数据 static data

静态数据指在联网汽车终端静态保存的数据。

3.4

运动数据 Dynamic data

动态数据是指在联网汽车不同的终端和服务器间进行传输的数据。

3.5

应用数据 Application data

应用数据指联网汽车终端运行的应用程序所产生的数据，如：用户账号密码，个人信息，服务数据等。

3.6

监控数据 Monitoring data

监控数据指负责监控联网汽车安全、状态的系统所产生的数据。

3.7

配置数据 Configuration data

配置数据指车联网系统各个终端的配置文件。

4 缩略语

下列缩略语适用于本文件。

CAN:控制器局域网(Controller Area Network)

OBD:车载诊断系统(On-Board Diagnostic)

TSP:汽车远程服务提供商(Telematics Services Provider)

PKI:公开密钥基础设施(Public Key Infrascture)

APN:接入点名称(Access Point Name)

VPN:虚拟专用网(Virtual Private Network)

IPS:入侵防御系统(Intrusion Prevention System)

IVI:车载信息娱乐系统(In-Vehicle Infotainment)

ECU:电子控制单元(Electronic Control Unit)

CRL:证书吊销列表(Certificate Revocation List)

OCSP:在线证书状态协议(Online Certificate Status Protocol)

HSM:加密模块(Hardware Security Module)

5 汽车联网系统架构

基于公众电信网的联网汽车信息安全技术要求主要由汽车网络架构安全技术要求、通信安全技术要求以及数据隐私安全技术要求三大部分组成。

联网汽车网络架构安全技术要求，主要包括汽车内部总线网络架构安全和连接公众电信网络架构的安全技术。

通信安全技术要求主要对联网终端、联网平台、联网客户端、通信技术、联网证书密钥管理技术的安全防护提出要求。

数据隐私安全技术要求主要对车联网系统中的数据进行了分类，并对不同类别的数据提出了相应的安全要求。联网汽车信息安全框架见图1。

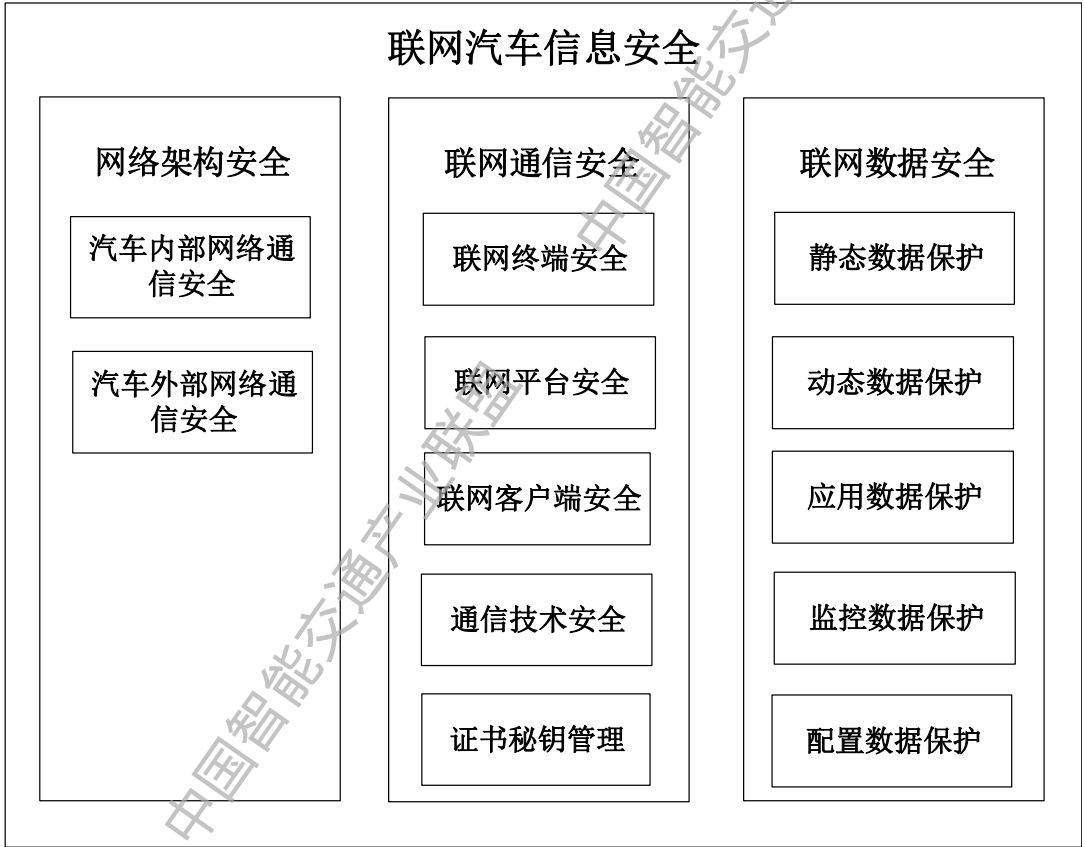


图 1 联网汽车信息安全框架图

6 联网汽车网络架构安全技术要求

6.1 联网汽车内部网络架构安全

- a) 应对采用汽车网关安全技术限制汽车总线内部不同功能的 ECU 之间访问，达到汽车 ECU 功能最小化控制权限，降低 ECU 被攻击后影响范围扩大的风险；（隔离）
- b) 应对汽车总线网络与外部通信接口之间应在 CAN 收发器模块内部使用 CAN 数据白名单的方式。限制外部通信设备对车辆内部总线网络的访问内容。防止通过汽车总线网络对外通信的接口对汽车控制模块进行攻击；（访问控制）
- c) 应在汽车网关中使用证书认证技术或认证校验算法，来验证汽车接入总线网络设备的合法性，防止未经授权的设备接入汽车总线对总线协议进行破解。（认证）
- d) 应对总线协议进行安全设计，使用加密算法（如 HMAC-MD5、HMAC-SHA1、HMAC-SHA256、HMAC-SHA512 等）对总线数据进行加密处理，或通过校验手段（如奇偶校验、添加校验和等）对总线数据进行安全校验，防止信息被窃听、重放攻击或恶意篡改；（加密）
- e) 应使用汽车车载 T-BOX、总线数据传输设备、汽车总线入侵检测模块，对总线传输报文进行实时的安全监控，并且上传至云端进行分析处理，对联网汽车综合安全信息进行态势分析和安全事件的预警。（监控）
- f) 应对汽车总线网络的状态、行为、数据变化进行安全审计，审计日志的保存时间应符合国家规定（六个月以上）；（审计）
- g) 应对汽车总线网络相关的设备、端口、文件等资产进行安全管理，消除安全隐患，做到事先防范和事后取证。（安全管理）

6.2 联网汽车外部网络架构安全

- a) 应对联网汽车接入的平台（TSP）以业务系统为最小单位进行安全域划分，并将控制车辆的系统做为最高安全级别系统，使用防火墙、ACL等基础访问控制手段与其它业务系统进行隔离，防止其它系统遭到入侵时影响车辆控制；（安全域划分）
- b) 应对要求对联网汽车接入网络进行隔离，以车辆为最小单位，使用PVLAN、虚拟隧道、ACL等网络隔离技术保障联网汽车之间不能进行通信。防止汽车遭到入侵后横向影响到其它联网汽车。（网络隔离、访问控制）
- c) 联网汽车与接入平台（TSP）进行通信时，应采用互联网协议安全标准（IPS）和安全可靠的接入方式如VPN、APN等，确保通信链路的保密性、可靠性，防止通信链路遭到信息泄露、窃取等；（传输加密）
- d) 联网汽车与接入平台（TSP）进行通信时，应采用PKI证书体系对联网汽车接入终端进行身份认证，建立合法的安全通信。防止通信链路遭到中间人攻击；（身份认证）
- e) 联网汽车应检测通过判断WIFI网络是否为开放式网络，检测WIFI网络内部是否存在嗅探行为，等措施验证接入WIFI网络的安全性，防止接入钓鱼WIFI而引发汽车劫持控制事件。
- f) 应针对联网汽车平台（TSP）远程管理时，采用VPN、SSH等可靠的远程安全管理方式进行远程管理，并且使用4A、堡垒机对远程管理人员进行审计和管理，防止黑客通过远程管理接口控制汽车。
- g) 应对联网汽车与接入平台网络进行实时安全监控，如发现异常流量、突发大量流量等事件进告警与响应，对联网流量的可用性、可靠性进行全方位的监控。保障联网汽车与平台网络之间联网状态平稳。（网络监控）
- h) 应对联网汽车接入平台的状态、行为、数据变化进行安全审计，审计日志的保存时间应符合国家规定。

7 联网通信安全技术要求

7.1 联网终端安全技术要求

7.1.1 OBD 安全技术要求

- a) 联网汽车OBD接口应采用白名单机制限制网络连接地址，并且通过使用芯片级访问控制措施限制OBD接口对车内信息的访问内容。防止攻击者通过OBD接口对汽车总线网络进行攻击；
(公网访问控制)
- b) 联网汽车OBD接口应采用证书或身份认证算法来确保接入OBD接口的设备为合法授权的设备，防止黑客通过未授权的OBD设备攻击汽车总线网络。(身份认证)
- c) 联网汽车OBD接口应对诊断功能及诊断协议的数据进行权限管理，限制非授权的OBD终端通过OBD接口下发诊断协议。

7.1.2 T-BOX 安全技术要求

- a) T-BOX应避免如JTAG、RS232、USB等敏感接口和引脚的暴露，减少固件被读取的风险，防止芯片内系统程序、终端参数、用户数据等被篡改或非法获取；
- b) T-BOX应采用硬件加密模块HSM，并确保硬件加密的加密运算执行和解密都在硬件内部实现，防止暴力破解和数据泄露；
- c) T-BOX应采取相应的固件保护措施（如：设置保护寄存器、写保护策略等），防止攻击者对固件的提取；
- d) T-BOX固件代码应采取相应的混淆措施、调整代码的层次结构，增加反汇编和固件逆向难度，提高固件的可靠性；
- e) T-BOX在固件升级时，应采用数字签名等技术确保升级文件的合法性，防止攻击者利用固件升级漏洞对固件进行刷写；应从指定的T-BOX固件库下载程序进行安全升级，禁止从非认证的固件库下载程序；升级失败要支持回退，确保固件升级的可靠性；
- f) T-BOX下发控制指令时应在CAN收发器中采用控制协议的白名单机制确保控制指令不被攻击者篡改下发其它控制指令到汽车总线。防止攻击者利用T-BOX攻击车身控制、动力控制系统；
- g) T-BOX应对用户数据、总线指令数据等敏感数据进行加密（如ISO29192中的轻量级密码算法:PRESENT等）存储，防止攻击者窃取敏感数据；
- h) T-BOX应设置操作日志，对数据的读、写、修改等操作进行记录，进行安全审计；
- i) 应对T-BOX状态进行监控，当车辆T-BOX被破坏或被非法拆去后，车厂后台应定位到汽车的VIN号等信息，及时限制或阻断汽车通讯信息并告警。

- j) 对T-BOX产生、传输、存储的数据按照本规范第八章相关规则进行分类，并根据第八章相应的数据安全保护要求进行保护；

IVI 安全技术要求

- a) IVI应避免USB、JTAG、RS232、等敏感接口和引脚的暴露，减少固件被读取的风险，防止芯片内系统程序、终端参数、用户数据等被篡改或窃取；
- b) IVI应采用硬件加密模块HSM，并确保硬件加密的加密运算执行和解密都在硬件内部实现，防止暴力破解和数据泄露；
- c) IVI应采取相应的固件保护措施（如：设置加密模块、保护寄存器、只读保护策略等），防止攻击者对固件的逆向和提取；
- d) IVI固件代码应采取相应的混淆措施、流程混排加密、代码内部字符串、调整加密的层次结构，提高反汇编和固件逆向难度，防止对固件进行反编译得到源代码；
- e) IVI在固件升级时，应采用数字签名等技术确保升级文件的合法性，防止攻击者利用固件升级漏洞对固件进行刷写；应从指定的IVI固件库下载程序进行安全升级，禁止从非认证的固件库下载程序；升级失败要支持回退，确保升级的安全性和可靠性；
- f) IVI应对其运行的应用程序有安全管理功能，如非授权应用程序安装防护、授权应用程序卸载防护、授权应用程序篡改防护，防止攻击者安装恶意程序和窃取合法程序等；
- g) IVI操作系统（如Android、QNX、Linux、YunOS等）应实现对IVI资源调用的监控、保护、提醒，确保涉及安全的系统行为总是处于受控状态下，防止出现用户不可控行为（如恶意代码攻击等）的执行；
- h) IVI操作系统应及时升级，并确保升级更新的可控性和安全性（如官方正版升级包等）；
- i) 对操作系统漏洞问题，应定期更新漏洞列表，及时修复系统漏洞和安装补丁，防止攻击者利用系统漏洞对IVI进行渗透；
- j) IVI应对总线控制程序的访问采用白名单等方式进行限制，防止攻击者利用IVI系统对汽车总线进行攻击；
- k) 对IVI产生、传输、存储的数据按照本规范第八章相关规则进行分类，并根据第八章相应的数
- l) IVI应对系统状态、行为、数据变化进行监控，检测异常行为并及时告警。

7.2 联网平台安全技术要求

- a) 保障TSP平台基础设备安全，需要对设备的物理端口、服务端口、硬件运行状态和系统性能等进行实时监控（如：视频监控、认证系统等），出现问题及时上报和处理，确保系统的稳定性和可靠性；
- b) TSP平台应进行安全域划分，并在边界部署防火墙或在核心交换机上配置防火墙模块、访问控制策略（如：IPS入侵防御系统、ACL访问控制列表等）实现访问控制；
- c) TSP平台应部署漏洞扫描系统或者恶意代码防护机制，定期检测服务器的操作系统、数据库系统配置等，识别安全隐患，评测安全风险，提供改进措施；
- d) TSP平台应利用黑白名单机制对通信接口进行访问控制，防止非法终端接入、非法数据注入等；
- e) TSP平台应采用专用安全通道（如VPN等）接入，车载终端与平台通信应进行双向安全认证；
- f) TSP平台与客户端的通信应全程使用HTTPS传输，并且强制使用；
- g) TSP平台应在边界部署WEB攻击防范设备，如WEB应用防火墙（WAF），实现对WEB攻击的检测和阻断，防止进行渗透测试、模糊测试、接口越权控制、SQL注入、XSS攻击、越权漏洞利用、暴力破解、文件上传漏洞利用、CSRF、DOS攻击等；
- h) TSP平台本地存储的数据（包括但不限于数据文件，日志文件、数据库文件、配置文件等）应采取加密方式（如DES、Rijndael等）保护存放敏感信息（如密钥、cookie、URL等）的文件；
- i) TSP平台应采用IDS对客户端传输的数据进行检测和过滤，并保证检测和过滤的全面性和有效性；
- j) TSP平台应对平台状态、行为、数据变化进行监控，检测异常行为并及时告警。

7.3 APP客户端安全技术要求

- a) APP客户端根据重要程度采取适宜的安全认证方式（如：“密码+验证码”，“密码+动态密码”，“密码+令牌等”）；
- b) APP客户端应用程序应对密钥/密码采取安全的存储保护方式（如哈希算法：SHA-512，加密算法：RSA-2048、AES-256）；
- c) APP客户端应用程序访问用户终端的权限应限制在程序实现自身功能的最低权限范围内，不应额外访问/读取本地其他文件获取用户信息；不应额外截获/记录/传输应用登录访问的敏感信息；不应访问非应用外internet访问及执行非许可的动作；

- d) APP客户端应对本地存储的数据（包括但不限于数据文件，日志文件，数据库文件、回话cookie等）采取加密方式保护存放敏感信息文件，对于关键数据，采用高强度加密算法（如：Triple等）加密算法，对于暂时存储的数据采用计算较快的加密算法（如DES加密算法等）；
- e) APP客户端信息传输应采用SSL/TLS数据加密传输方式，并在客户端对SSL证书和发行进行校验；信息传输全流程使用HTTPS加密，且是强制使用；
- f) 客户端程序应通过对代码的高级混淆、流程混排加密、代码内部字符串加密等，对源码、函数名称以及接口调用进行加密隐藏，防止第三方对应用程序进行反编译。
- g) APP客户端程序应在启动和更新时进行真实性和完整性校验，防范客户端程序被篡改（如通过计算crc32或哈希值的方法对整个apk的真实性和完整性进行校验）。

7.4 通信技术安全技术要求

7.4.1 APN 安全技术要求

- a) 运营商应提供专享的APN鉴权接入（只有符合TSP平台专用APN域名的无线卡才能接入，域名的申请和绑定都需要经过规定的流程）；
- b) 运营商应使用专用行业专用网关，并由网关判断APN用户的合法性，与互联网网关互相独立；
- c) APN专网数据传输应全部经过GTP隧道封装，防止数据在传输过程中被窃取；
- d) APN专网应支持GRE/L2TP隧道接入方式，并支持多种安全加密方式（如增强的128位鉴权密码算法、KASUMI分组加密算法等）对传输数据进行加密，防止消息被恶意篡改和伪造；
- e) TSP平台内网应采用鉴权方式，对每个拨入的号码进行账号和密码认证，TSP平台内网可自行分配IP地址和拨入服务器主机IP地址和域名；
- f) TSP平台可以在其内网部署防火墙设备，对不同网络间的通信进行限制或隔离处理，将APN网络系统受外界影响的风险降到最低。

7.4.2 VPN 安全技术要求

- a) 标识：在用户对VPN资源访问之前，对用户进行标识，监控用户行为；具体参照《信息技术VPN产品安全检验规范 MSC-GFJ-03》；
- b) 鉴别：在远程访问VPN中，在VPN隧道建立前对远程用户进行鉴别，当用户对VPN 资源访问之前，对提出该动作要求的用户身份通过MAC地址、IP地址、数字证书等进行身份鉴权；
- c) 审计事件：为可审计事件生成审计记录，审计事件包括：用户鉴别失败事件，VPN隧道建立和删除，用户数据解密失败等；
- d) 访问控制：利用访问控制表对VPN系统的资源进行访问控制，用户对VPN资源的访问权限对应一张访问控制表，用以表明用户对VPN资源的访问能力；

- e) VPN专用网络间数据传输保护：当数据在VPN专用网络间传输时，虚拟专用网设备应根据预定的安全策略数据库中定义的规则对数据进行加密保护；当未建立隧道时，通过手工设定密钥及安全关联参数，根据协商的密钥等参数对数据进行加密保护；
- f) 专用网络向公用网络输出数据的保护：应根据预先在配置文件如安全策略数据库中对输出数据类型的安全属性设定的策略和敏感标记，确定是否需要加密等保护或直接转发、丢弃等；
- g) 公用网络向专用网络输出数据的保护：应根据预先在配置文件如安全策略数据库中对输入数据类型所设定的敏感标记和策略进行处理，从隧道中提取原始数据并进行解密，并将数据转发至专用网内正确的目的主机中。

7.4.3 eSIM 安全技术要求

- a) eSIM和运营平台之间的通信必须进行双向认证，防止重放攻击；
- b) eSIM和运营平台之间应协商一套最小的公共机密工具集进行端到端的认证、完整性保护和一致性保护；
- c) eSIM应不得向任何未经认证的服务器提供私密数据；
- d) eSIM应对Profile(运营商数据)进行加密，确保Profile明文仅存在于服务器和eSIM内部，防止Profile数据泄露；
- e) eSIM应进行安全域划分，对安装到eSIM中的多个Profile进行隔离，防止Profile数据失效；
- f) eSIM下载数据之前，用户应输入正确的口令（确认码），防止Profile被非法用户窃取。

7.5 证书密钥管理技术要求

7.5.1 PKI

- a) 进行PKI系统硬件设备、相关环境和系统安全的设计时，应按照 GB/T 21052—2007 第 4 章所描述的要求；
- b) PKI系统部件密钥和系统用户密钥生成应由相应级别的 CA（建议车厂自建CA）或 RA 等机构进行，可用软件方法产生，生成算法和密钥长度等应符合国家密码行政管理部门的规定；
- c) 如果终端用户自己生成密钥对，终端用户应将公钥安全的提交CA，如使用证书载体等方法进行面对面传送；
- d) CA向用户传送与分发私钥应以加密形式进行，加密算法等应符合国家密码行政管理部门的规定；
- e) CA签名私钥应存储于国家密码行政管理部门规定的密码模块中或由硬件密码设备加密后存储，终端用户密钥由用户自行存储；
- f) PKI系统所签发的公钥证书应与GB/T 20518-2006相一致，任何证书所包含的字段或扩展应被 PKI系统根据GB/T 20518-2006生成或经由颁发机构验证以保证其与标准的一致性；
- g) 发布 CRL 的 PKI 系统应验证所有强制性字段的值符合 GB/T 20518-2006，发布 OCSP 响应的 PKI 系统应验证所有强制性字段的值符合 GB/T 19713-2005；
- h) 应按 GB/T 20271-2006 中 6.1.5.1 的要求，在配置管理能力方面实现对版本号等方面的要求；
- i) 应按 GB/T 20271-2006 中 6.1.5.2 的要求，实现 PKI 系统的分发和操作。

备注：PKI 参考 GB/T 21053—2007 信息安全技术 公钥基础设施 PKI 系统安全等级保护技术要求。

7.5.2 加密算法

- a) 应尽量采用国产加密算法（如对称算法SM4、非对称算法SM2、哈希算法SM3等）对数据进行加解密处理，以保障应用和数据的存储、传输和使用安全；
- b) 应将用户密码与其它用户识别信息（如用户帐号或其它注册信息）采用哈希算法进行处理后作为用户鉴别信息的哈希值存储，以保证每个用户的鉴别信息不同；
- c) 保障数据保密性，防止用户的标识或数据被读取，例如采用对称算法（如SM4等）对数据进行加密处理后进行传输或存储，算法处理中使用的对称算法密钥通过其它安全方式进行传输或存储；
- d) 保障数据完整性，例如采用哈希算法对重要业务数据生成数字摘要、添加时间戳信息等防止数据被篡改。

8 联网数据隐私安全技术要求

8.1 静态数据安全保护要求

- a) 根据已确定的静态数据处理目的和各业务场景，确定静态数据存储期限，确保静态数据存储期限为实现目的所必需的最短时间，法律法规另有规定的除外；
- b) 静态数据的存储，应采用加密等安全措施；
- c) 存储静态数据时，应采取匿名化或去标识化措施，法律法规另有规定的除外；
- d) 对可访问静态数据的对象，应确保最小授权，使其仅具备完成职责所需权限且只能访问职责所需的最少够用的静态数据，并对权限管理建立追责和溯源机制；
- e) 对静态数据的存储、访问、修改等活动设定相应的权限、审批和管理流程；
- f) 对静态数据进行备份和完整性检测，静态数据遭到破坏时，应及时告警，并且采取相应的数据恢复措施。

8.2 运动数据安全保护要求

- a) 根据已确定的运动数据处理目的和各业务场景，确定运动数据存储期限，确保运动数据存储期限为实现目的所必需的最短时间，法律法规另有规定的除外；
- b) 运动数据的存储，应采用加密等安全措施；
- c) 利用黑白名单限制发送终端的接入，确保传输动态数据的终端真实可信，防止设备的非法接入；
- d) 对运动数据进行本地备份和完整性检测，及时发现运动数据在被传输的过程中被篡改、删除、插入情况，并在检测到完整性错误时发出警告并对数据进行重传；
- e) 对动态数据进行安全审计，发现违规动态数据应及时告警。

8.3 应用数据安全保护要求

- a) 应根据应用数据的分类和功能设置限制用户对应用数据的访问，只有获得相应的访问权限才可以对应用数据文件进行操作，如读、写、删、改等；
- b) 应对联网客户端应用数据的访问进行监测，若对应用数据的访问发生异常行为，则应阻止该访问操作继续进行，发出告警，记录日志，并锁定系统。
- c) 应对联网平台应用数据的访问行为检测，针对不同用户设置访问权限，当检测到有用户进行越权访问数据时，应立即阻止该操作的进一步执行，恢复被篡改的数据，发出告警，记录日志，并锁定该用户访问系统权限。

- d) 用户鉴别信息应采用用户口令+用户账号的哈希值存储以保证其唯一性和保密性;
- e) 应采用HTTPS加密协议对客户端和服务端间的通信数据进行加密传输;
- f) 应对应用数据进行定期的备份, 如果检测到数据异常、篡改、删除等情况, 则采取相应措施恢复数据。

8.4 监控数据安全保护要求

- a) 监控数据只允许在服务器端存储, 禁止在客户端以及其它区域存储, 防止攻击者从客户端得到监控数据;
- b) 对服务器端存储的监控数据进行隔离: 对每个汽车产生的监控数据和指令分配独立的内存空间, 以防止监控数据被非法访问;
- c) 客户端向服务器传输监控数据的通信应在服务器的控制下进行, 服务器应对监控数据提供方的身份进行判断, 以决定是否允许其进行通信;
- d) 应保证只有授权管理员和可信主机才有权使用产品的管理功能, 具备对授权管理员和可信主机进行身份鉴别的功能;
- e) 应对数据源所产生的监控数据进行实时监视, 并能对汽车异常情况发出告警。

8.5 配置数据安全保护要求

- a) 应将联网客户端中的配置数据存放于不可更改的存储空间内;
- b) 应将配置数据和应用数据、监控数据、活动数据存储于不同的存储空间;
- c) 应对重要配置数据采用对称算法(如SM4等)进行加密存储;
- d) 应利用黑白名单限制配置数据的访问权限, 非系统开发人员不能访问、修改配置数据;
- e) 移动终端应能够检测出存储在移动终端内的数据是否被篡改, 以防止出现非法修改存储数据的攻击。

中国智能交通产业联盟

标准

基于公众电信网的联网汽车信息

安全技术要求

T/ITS 0068-2017

北京市海淀区西土城路 8 号（100088）

中国智能交通产业联盟印刷

网址：<http://www.c-its.org>

2017 年 12 月第二版 2017 年 12 月第一次印刷