ICS 35.100
L 79

T/ITS

中国智能交通产业联盟标准

T/ITS 0035—2015

合作式智能运输系统

信息安全总体技术要求

General Security Requirements of Cooperative ITS

2015-11-23 发布　　2016-01-01 实施

中国智能交通产业联盟　发布

目　　次

前　言

本标准按照GB/T 1.1-2009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。

本标准于2015年11月首次发布，本次为首次发布。

本标准主要起草单位：电信科学技术研究院、交通运输部公路科学研究院、中国信息通信研究院、华为技术有限公司、交通运输部信息通信及导航标准化技术委员会、北京车网互联科技有限公司、北京握奇智能科技有限公司、戴姆勒大中华区投资有限公司、深圳市金溢科技股份有限公司、紫光捷通科技股份有限公司、大众汽车(中国)投资有限公司。

本标准主要起草人：徐晖、周巍、宋向辉、杨文丽、葛雨明、韩广林、应江威、江伟、王义锋、段起志、程朝辉、张伟、吴嘉谊、周迅、赵闻。

引　言

为使合作式智能运输系统信息安全能够按统一的标准进行说明和描述，特制定本标准。

为了保持标准的适用性与可操作性，各使用者在采标过程中，及时将对本标准规范的意见及建议函告电信科学技术研究院，以便修订时研用。

地址：北京市海淀区学院路 40 号，邮编：100191，邮箱：xuhui@catt.cn。

合作式智能运输系统 信息安全总体技术要求

1 范围

本标准主要针对合作式智能运输系统的信息安全进行研究，提出了合作式智能运输系统信息安全总体技术要求，针对合作式智能运输系统中的车载设备、路侧设备、出行者设备、中心设备、通信服务和应用服务提出了相应的安全技术要求。

本标准适用于合作式智能运输系统中的车载设备、路侧设备、出行者设备、中心设备、通信系统和应用系统的信息安全。

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 4943.1-2011 信息技术设备安全

YD/T 1754-2008 电信网和互联网物理环境安全等级保护要求

3 缩略语

下列缩略语适用于本文件。

DOS：拒绝服务（Denial of Service）

EAP-PEAP：扩展的认证协议-保护的 EAP（Extensible Authentication Protocol-Protected EAP）

EAP-SIM：基于 SIM 卡的扩展认证协议（Extensible Authentication Protocol- Subscriber Identity Module）

IPsec：协议安全性（Internet Protocol Security Internet）

MAC：媒体介入控制层（Media Access Control）

NTP：网络时间协议（Network Time Protocol）

OBU：车载单元（On board Unit）

RSU：路侧单元（Road Side Unit）

SNMP：简单网络管理协议（Simple Network Management Protocol）

SPI：全状态数据包检测（Stateful Packet Inspection）

SSH：安全外壳协议（Secure Shell）

SSL：安全套接层（Secure Sockets Layer）

TLS：传输层安全（Transport Layer Security）

URL：统一资源定位符（Uniform Resource Locator）

WEP：有线等效保密（Wired Equivalent Privacy）

WPA：网络安全接入（Wi-Fi Protected Access WIFI）

WAPI：无线局域网鉴别和保密基础结构（Wireless LAN Authentication and Privacy Infrastructure）

4 概述

4.1 系统架构

合作式智能运输系统由车载子系统、路侧子系统、中心子系统和出行者子系统构成。

a) 车载子系统：包括OBU,车载网关、和路由器等；

b) 路侧子系统：包括RSU，路侧网关、路由器、边缘路由器等；

c) 中心子系统：包括中心解密、中心交换、服务组件节点、服务路由器和中心接入节点等，具备网络管理、业务支撑等能力；

d) 出行者子系统:由出行者所携带的各类信息终端及其他信息处理设备构成。

合作式智能运输系统的不同对象之间的通信关系见图 1。

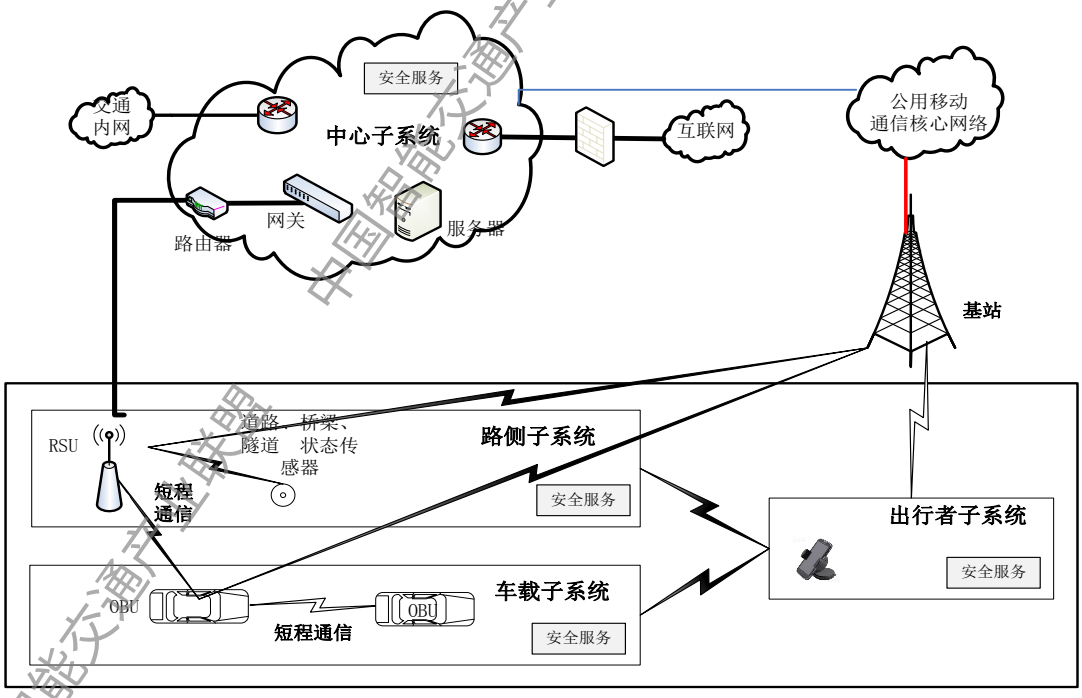

图 1 合作式智能运输系统架构

合作式智能运输系统安全服务子系统存在于中心子系统、车载子系统、路侧子系统和出行者子系统中，并为这些子系统提供数据安全、应用安全、网络安全、主机安全、物理安全和管理安全等服务。服务所涵盖的内容如下：

a) 数据安全：对数据传输、存储、查看、分析处理等方面的安全要求，同时涉及数据备份恢复等

方面的要求；

b) 应用安全：合作式智能运输系统的应用程序的安全，包括服务商或用户开发的应用程序；

c) 网络安全：合作式智能运输系统的网络安全，包括安全域划分、访问控制、安全边界防护和攻击防范等方面；

d) 主机安全：合作式智能运输系统的各类服务器的安全，包括安全配置与加固、访问控制、攻击防范、恶意代码防范等方面；

e) 物理安全：合作式智能运输系统设备及其所处环境设施的安全保护和控制；

f) 管理安全：安全管理的各项措施要求。

4.2 安全架构

合作式智能运输系统安全服务架构分为三个层次。

a) 安全功能层：包含一组安全功能，提供合作式智能运输系统所需的各种安全服务。这些安全服务可分为网络安全、密码安全、访问控制、操作安全、物理安全和管理安全等六个大类；

b) 安全环境抽象层：该层实现与安全环境相关的各种安全能力，诸如密钥分散、数据加密与解密、数字签名生成与验证和安全凭证的读写等。该层还提供对安全环境的物理访问能力；

c) 安全环境层：该层提供与敏感数据存储与敏感功能执行相关的能力。敏感数据包括密钥、安全凭证、安全策略、身份信息和签约信息等。敏感功能包括数据加密、数据解密和密钥生成等。

合作式智能运输系统安全服务架构见图 2。

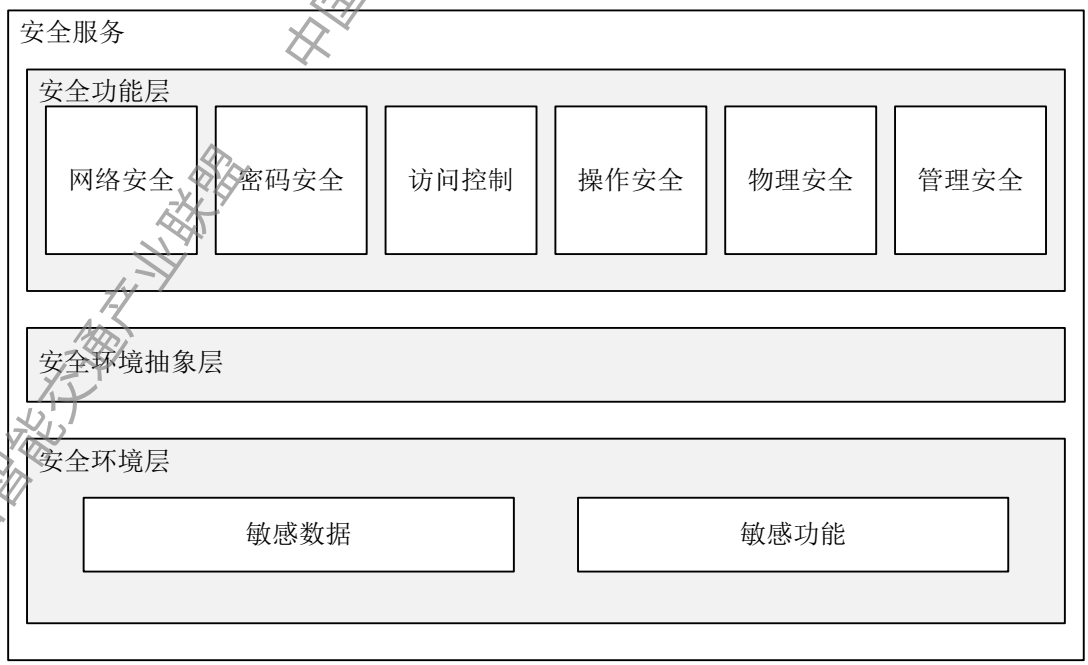

图 2 合作式智能运输系统安全服务架构

安全功能层提供的主要功能为：

a) 网络安全：保护和监控非授权访问、使用、修改或拒绝访问网络资源，具体应提供防火墙、防病毒、漏洞扫描和入侵防御等功能；

b) 密码安全：提供数据的机密性、完整性、认证性和不可否认性等功能，具体应提供数据的加密和解密、密钥管理、数字签名与验证、公钥基础结构、通信安全和隐私保护等功能；

c) 访问控制：防止对资源的未授权访问，并确保合法用户对资源的访问，具体应提供认证、授权、账户管理、会话管理和错误处理等功能；

d) 操作安全：确保业务连续性的操作，具体应提供安全监控、数据备份、事故响应与恢复、数据恢复和安全审计等功能；

e) 物理安全：确保移动和固定设备的物理安全，具体包括用于存储敏感数据与执行敏感功能的基于硬件的安全环境、设备的防篡改机制、电源安全和存储介质安全等；

f) 管理安全：提供密钥及证书生成、密钥及证书写入和更新，软件更新和敏感数据写入等功能。

5 车载设备安全总体技术要求

5.1 安全保护原则

车载设备安全总体技术要求应保障车载设备在车辆行驶、静止等多个状态下的安全。

车载设备安全总体技术要求包括车载设备安装环境的物理安全技术要求，以及车载设备在使用过程中的信息安全技术要求。

5.2 安全技术要求

5.2.1 车载设备物理安全技术要求

车载设备按照车载电子设备应符合 GB 4943.1-2011《信息技术设备安全》的规定。

车载通信设备应具备整机防盗、SD 卡、SIM 卡防盗功能。

5.2.2 车载设备信息安全技术要求

车载设备应支持：

a) 防火墙功能，包括 SPI 过滤、MAC 过滤、IP 地址过滤、URL 过滤中的一种或多种，以及服务访问控制、DOS 防护、安全策略高级特性；

b) 不加密、静态 WEP 加密、WPA、WPA2、WAPI 中的一种或多种加密方式；

c) Portal 认证，MAC 认证，EAP-SIM 认证，EAP-PEAP 中的一种或多种认证方式；

d) 运营和服务信息的 IPSEC 加密安全传输，不与普通上网数据混合；

e) 对业务数据按照重要性进行分类管理，按类别进行读写和删除的操作授权；

f) 保证自身的位置和时钟不被篡改。

6 路侧设备安全总体技术要求

6.1 安全保护原则

安全保护原则应满足：

a) 对路侧设备进行身份认证，并确信设备是否完好；
b) 接入路侧设备用户的身份及其真实性；
c) 路侧设备内部、路侧设备和车载设备之间、路侧设备和数据中心之间的数据安全，具备安全数据（完成安全功能所需要的数据，如用户身份和口令）的保护能力；
d) 对用户对资源的使用进行控制，不允许用户过量占用资源造成的拒绝服务；
e) 提供日志等审计记录，这些记录可以用来分析安全威胁活动和对策；
f) 根据数据类型建立不同的传输路径，对于传送敏感数据的通信要同传送其他数据的通信隔离开来。

6.2 安全技术要求

6.2.1 信源层安全

路侧设备应支持：

a) 保证物理安全，应符合 YD/T 1754-2008《电信网和互联网物理环境安全等级保护要求》的规定；
b) 采用认证协议对路侧设备进行定时认证；
c) 对各类信息进行有效的分类处理，同一类的信息实行统一安全通信协议、加密和签名等技术进行安全保障；
d) 建立对数据进行数字签名和数据完整性验证的协议，确保信息数据完整可信。

6.2.2 集群安全

路侧设备应支持：

a) 对所有路侧设备布设防病毒软件和防火墙，对访问路侧设备设置用户权限管理；
b) 采用设备监控措施对路侧设备性能、物理端口、服务端口和硬件运行状态等进行实时监控，出现问题及时上报和处理，保障路侧设备的稳定性和可靠性；
c) 集成远程监控和报警机制对路侧设备进行全天 24 小时远程监控。

6.2.3 网络传输安全

网络传输应支持：

a) 建立 IpSecS 隧道加密和无线隧道加密技术体系，对路侧设备和数据中心之间、路侧设备和车载设备之间的数据进行加密传输，防止数据被非法篡改改和截获；
b) 路侧设备可以通过访问控制列表进行远端网络访问控制，访问控制列表是基于报文的内容（如 IP 地址等）指定的安全规则表，对每个进出路侧设备的报文通过与这些规则匹配，确定对其处理动作。

6.2.4 系统安全

系统安全应满足：

a) 对路侧设备运行状况、网络流量、用户行为等进行日志记录；
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
c) 采用技术手段，保证所有网络设备的系统时间自动保持一致；
d) 对审计记录进行保护，避免受到未预期的删除、修改或覆盖等；
e) 在路侧设备存储备份区部署漏洞扫描系统，定期检测数据库系统配置，识别安全隐患并实施安

全加固；

f) 对路侧设备部署防病毒系统，防止系统遭受来自外部或内部的病毒、恶意代码、木马等攻击。

6.2.5 应用安全

应用安全应满足：

a) 路侧设备的以太网接口应由一个可配置的防火墙保护；

b) 采用 SSL 加密、CA 认证等技术，保证敏感数据的安全传输；

c) 对用户的身份和授权统一定义，每个用户只能允许访问经过确认的业务应用服务和设备；

d) 进行软件代码安全性审核，对路侧设备运行软进行实践性的安全检测。

6.2.6 安全管理

安全管理应满足：

a) 路侧设备由一个符合本地安全策略的密码来保护；

b) 对路侧设备的配置文件进行哈希计算以便容易地识别未经授权的修改；

c) 路侧设备的本地文件系统应被加密；

d) 对于路侧设备可以使用以下远程管理方式：

- SNMP：应支持 SNMPv3 等安全机制
- 远程登录：建议支持 SSHv1 和 SSHv2，通过认证算法和加密算法实现对管理设备数据的保密性和完整性保护
- Web 管理：可通过支持 SSL/TLS 安全协议，实现对管理用户数据的完整性保护

6.2.7 时钟同步

安全管理应满足：

a) 当路侧设备失去 GPS 定位时，应与一个 NTP 服务同步系统时钟；

b) 当使用 NTP 服务同步时钟时，应对从 NTP 服务器接收到的信息进行认证。

7 出行者设备安全总体技术要求

7.1 安全保护原则

出行者设备包括智能终端等设备，其安全保护原则包括：

a) 整体性原则：任何硬件和软件的安全漏洞都可能导致出行者设备受到安全威胁，同时，出行者设备的硬件和软件作为有机整体相互关联，因此出行者设备的信息安全应从整体的角度来全面考虑；

b) 相对性原则：出行者设备的信息安全应适度，不能偏离实际情况而片面追求绝对安全，应采用分类分级的方法针对性提高出行者设备信息安全能力；

c) 目的性原则：出行者设备的信息安全设计应有目标、有重点地实施，需要对出行者设备信息安全进行一定程度分类，有重点加强出行者设备信息安全；

d) 扩展性原则：出行者设备的信息安全形势以及对应安全技术是不断发展的，在一段时期内，信息安全发挥了其应有的作用，达到一定平衡，但一旦有安全攻击技术超越安全防护，新的安全周期就要重复开始。因此出行者设备信息安全应具备充分的扩展性；

e) 易用性原则：出行者设备的主要特点就是人机友好、易于掌握和使用灵活，安装卸载应用软件方便，任何信息安全措施都不能严重影响出行者设备的易用性。故此，出行者设备的信息安全措施基于其易用性，达到安全性和易用性的平衡。

7.2 安全技术要求

7.2.1 硬件安全要求

出行者设备的硬件要确保系统程序、设备参数、安全数据、用户数据不被篡改或非法获取。

7.2.2 操作系统安全要求

出行者设备的操作系统安全要达到操作系统对系统资源调用的监控、保护、提醒，确保涉及安全的系统行为总是在受控的状态下，不会出现用户在不知情情况下某种行为的执行，或者用户不可控的行为的执行。

另外操作系统还应保证自身的升级是受控的。

7.2.3 外围接口安全要求

出行者设备的外围接口要确保用户对外围接口的连接及数据传输的可知、可控。

7.2.4 应用层安全要求

出行者设备的应用层要保证出行者设备对要安装在其上的应用软件可进行来源的识别，对已经安装在其上的应用软件可以进行敏感行为的控制。另外还要确保预置在出行者设备中的应用软件无损害用户利益和危害网络安全的行为。

7.2.5 用户数据保护安全要求

出行者设备要保证用户数据的安全存储，确保用户数据不被非法访问、不被非法获取、不被非法篡改，同时能够通过备份保证用户数据的可靠恢复。

8 中心设备安全总体技术要求

8.1 安全保护原则

中心设备安全保护原则应包括：

a) 数据安全：主要包括数据一致性保护、安全审计、不良信息清除、版权保护、备份数据安全等方面的安全要求；
b) 业务系统安全：主要包括中心系统的结构安全、访问控制、入侵防范、请求路由系统安全以及冗余系统、冗余设备、冗余链路等方面的安全要求；
c) 基础设施安全：主要包括主机安全、物理资源安全、网络及安全设备防护等方面的安全要求；
d) 管理安全：主要包括人员和技术支持能力、运行维护管理能力、灾难恢复预案等方面的安全要求。

8.2 安全技术要求

8.2.1 身份鉴别认证

身份鉴别认证应满足：

a) 应对登录操作系统和数据库系统的用户进行身份标识和鉴别；
b) 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；
c) 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
d) 应根据业务需要，采用安全方式防止用户鉴别认证信息泄露而造成身份冒用；
e) 当对服务器进行远程管理时，应采取加密措施，防止鉴别信息在网络传输过程中被窃听；
f) 应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性。

8.2.2 访问控制

访问控制应满足：

a) 应采用技术措施对合法访问终端的地址范围进行限制；
b) 应关闭系统不使用的端口，防止非法访问；
c) 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限。

8.2.3 安全审计

安全审计应满足：

a) 审计范围应覆盖到服务器上的每个操作系统用户和数据库用户；
b) 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；
c) 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；
d) 应保护审计记录，避免受到未预期的删除、修改或覆盖等。

8.2.4 资源控制

资源控制应满足：

a) 应通过设定终端接入方式、网络地址等条件限制终端登录范围；
b) 应根据安全策略，设置登录终端的会话数量；
c) 应根据安全策略设置登录终端的操作超时锁定；
d) 应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况。

8.2.5 恶意代码防范

恶意代码防范应满足：

a) 应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；
b) 应支持防恶意代码软件的统一管理。

8.2.6 入侵防范

入侵防范应满足：

a) 操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，保持系统补丁及时得到更新。
b) 应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；
c) 应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施。

9 通信服务安全总体技术要求

9.1 安全保护原则

通信服务应该支持以下的原则：

a) 机密性：需要保证通信网络的数据传输的机密性；
b) 完整性：需要保证物联网通信网络的数据传输的完整性；
c) 可认证性：可以采用多种认证方式保证通信双方的可信性和合法性；
d) 可用性：确保通信网络的信息和服务在任何时间都可以提供给合法用户；
e) 不可否认性：保证通信各方对自己行为及对行为发生的时间的不可抵赖性；
f) 审计性：审查通信服务的安全性、可靠性、可用性、保密性等。

9.2 安全技术要求

9.2.1 网络安全技术安全

9.2.1.1 网络拓扑结构安全

网络拓扑结构安全应满足：

a) 应绘制与当前运行情况相符的网络拓扑结构图，便于网络管理；
b) 应保证关键网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；
c) 应保证接入网络和核心网络的带宽满足业务高峰期需要；
d) 应根据合作式智能运输系统的服务类型、功能及服务租户的不同划分不同的子网或网段，并依据方便管理和控制的原则为各子网、网段分配地址段；
e) 应按照用户服务级别协议的高低次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护高级别用户的服务通信。

9.2.1.2 访问控制

访问控制应满足：

a) 应在(子)网络或网段边界部署访问控制设备，启用访问控制功能；
b) 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力；
c) 应在会话处于非活跃一定时间或会话结束后终止网络连接；
d) 应限制网络最大流量数及网络连接数。

9.2.1.3 安全审计

安全审计应包括：

a) 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
c) 应采用技术手段，保证所有网络设备的系统时间自动保持一致；
d) 应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。

9.2.1.4 入侵防范

入侵防范应满足：

a) 应在网络边界处监视以下攻击行为：端口扫描、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；
b) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警；
c) 应周期性地对攻击、威胁的特征库进行更新，并升级到最新版本。

9.2.1.5 网络设备防护

网络设备防护应满足：

a) 应对登录网络设备的用户进行身份鉴别；
b) 应对网络设备的管理员登录地址进行限制；
c) 网络设备用户的标识应唯一；
d) 身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换；
e) 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；
f) 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；
g) 应对网络设备进行分权分域管理限制默认用户或者特权用户的权限，做到最小授权。

9.2.2 短程通信安全技术要求

短程通信安全应满足：

（1）与机密性相关的安全技术要求：

a) 设备发送和接收的数据不能泄露给任何未被授权的用户；
b) 设备内的数据不能泄露给任何未被授权的用户；

c) 用户的身份信息和设备提供服务的能力不能泄露给任何未被授权的第三方；
d) 防止对发送给设备或从设备接收的管理数据的非法访问；
e) 防止对设备内的管理数据的非法访问；
f) 非授权用户不可能通过分析通信数据流而推导出设备用户的位置和身份信息；
g) 非授权用户不可能通过分析设备的通信数据流而推导出其行驶的路径。

（2）与完整性相关的安全技术要求：
a) 设备内的信息不应当未经授权而被修改和删除；
b) 应防止从注册设备用户发出或接收来自于注册设备用户的信息在传输过程中被未经授权或恶意地修改或操作；
c) 应防止设备内的管理信息在未经授权的情况下被修改和破坏；
d) 应防止从设备发出或接收来自于设备的管理信息在传输过程中被未经授权或恶意地修改或操作。

（3）与认证性相关的安全技术要求：
a) 防止非授权的设备假冒一个合法设备与另一个合法设备进行通信；
b) 设备不可能从非授权用户那里接收和处理与管理和配置相关的信息；
c) 只有授权的设备才能获得那些受限制的服务。

（4）与可用性性相关的安全技术要求：
授权用对系统服务的访问或操作不应被恶意行为所阻拦。

（5）与审计性相关的安全技术要求：
审计系统可以监控和记录对安全参数和应用系统的所有操作（修改、增加和删除）。

9.2.3 移动蜂窝网安全技术要求

移动蜂窝网安全应满足：
a) 对移动蜂窝网络中通信的节点进行双向认证和业务授权；
b) 采用完善的密码技术，利用当前比较成熟的密码体制以及密钥管理制度（例如,基于密钥基础设施 PKI 的安全机制或者基于对称密钥协商的安全机制等），对端到端、节点到节点的数据都进行合理的完整性保护；如有需求，还需要对某些敏感数据进行加密保护；
c) 要考虑不同网;络中的认证和密钥协商机制不同,解决跨网认证和跨域认证对安全的不利因素；
d) 在多播或者广播情况下确保信息的安全传输。

10 应用服务安全总体技术要求

10.1 安全保护原则

在合作式智能交通运输系统中，应用大致可以分为生命安全类应用和非生命安全类应用两大类（以下简称安全应用和非安全应用）。在安全应用中，车辆通常周期性广播信标帧，其中包括车辆自身的位置、速度、加速度以及其他车辆状态数据。这些数据的预期接收者是附近能够直接进行通信的邻居车辆，用途是对潜在的危害行驶安全的状况进行检测。而非安全应用关注的主要是提供大型数据传输和提供各种服务。因此二者对信息安全保护的要求也不尽相同，下面分别进行阐述。

10.1.1 生命安全类应用安全保护原则

（1）信息的及时性

对于安全应用而言，获取信息及时性是一个必备的前提条件，因此对系统的处理延迟有严格的要求，车辆广播自身位置、速度等信息的频率均为 100ms，系统中延迟超过 100ms 的数据通常被

认为是无效的。因此，在实现对通信的安全保护时，必须保证不能引入过大的处理延迟。

（2）信息的非机密性

在安全应用中，通信的主要内容是车辆的位置、速度等信息。对于在合作式智能交通运输系统中的每一个交通参与方而言，在一定范围内（通常是在其无线短程通信覆盖区域内），这些信息是公开的，不具有机密性的，周围的交通参与者都可以通过接收广播消息来获得这些信息。

（3）信息的真实性和完整性

在安全应用中，保证信息的真实性和完整性至关重要。正是由于信息的非机密性，交通系统中所有参与者都可以轻易的获取周边车辆的位置、速度等信息。如果恶意攻击者伪造和篡改消息车辆发出的信息，则会在周边的道路交通带来很大的安全隐患。因此，应在系统中提供对消息的真实性和完整性的验证机制。

（4）信息的有效性

在安全应用中，仅保证了信息内容的真实和完整，不一定能确保信息一定真实的。在一种网络攻击中，恶意攻击者可以将接收到的消息在另外的时间或位置进行重放，伪造道路的交通状况，从而对车辆的通行安全带来潜在威胁。因此，保证信息的有效性（时效性）也是信息安全的一个重要的方面。

（5）隐私性

隐私是安全应用的核心需求之一。在整个交通系统中，车辆需要周期性的广播自身的位置、速度等信息，这些信息可以被用来跟踪车辆，收集到的车辆运行轨迹还可能被提供给第三方以未预期的方式使用。这都将导致车辆驾驶者的隐私被侵犯。

10.1.2 非生命安全类应用安全保护原则

非生命安全类应用安全保护原则包括：

a) 只有合法用户才能使用非生命安全类应用服务提供商提供的服务，用户的使用本身也是合法的、合乎要求的；
b) 非生命安全类应用服务提供商在用户使用业务时为用户提供隐私保护；
c) 为了保证可用性和业务的连续性，非生命安全类应用服务提供商一方面防止用户未经请求而访问，另一方面保证第三方的业务被安全地送达；
d) 对安全事件可控，或者恢复正常状态，或者能把损失减到最小；
e) 所施加的安全措施和机制不能影响业务质量，应综合考虑性能、可用性、可升级、成本代价；
f) 只有经授权的非生命安全类应用提供商和用户才能在授权的范围内检索与之相关的服务的安全信息。

10.2 安全技术要求

10.2.1 身份认证

身份认证应满足：

a) 应采用静态密码、数字证书、智能卡、手机短信、随机密码器等方式，对公有云应用系统或服务的用户进行身份认证；
b) 对应支持提供用户访问日志记录，记录用户登录信息，包括系统标识、登录用户、登录时间、登录 IP、登录终端等标识。

10.2.2 访问控制

访问控制应满足：

a) 应提供专用的登录控制模块对登录用户进行身份标识和鉴别；对用户账号、口令、密码、身份标识等重要信息应加密存储；

b) 应支持用户单点登录，并可设置单点登录的最长会话时间、最长空闲时间、最长高速缓存时间等；

c) 应支持通过采用基于身份认证的权限控制方式，进行实时的身份监控、权限认证和证书检查，禁止租户之间的非授权访问，防止用户间的非法越权访问。

10.2.3 安全审计

安全审计应满足：

a) 审计范围应覆盖到用户的关键操作、重要行为、业务资源使用情况等重要事件，如普通用户异常登录、发布恶意代码、异常修改帐号信息等行为；

b) 应保护审计记录，保证无法删除、修改或覆盖等。

10.2.4 资源控制

资源控制应满足：

a) 应限制对应用访问的最大并发会话连接数及资源配额；

b) 应提供资源控制不当的报警及响应。

10.2.5 恶意代码防范

恶意代码防范应满足：

a) 应对恶意代码进行检测和清除；

b) 应维护恶意代码库的升级和检测系统的更新。

10.2.6 生命安全类应用的安全要求

生命安全类应用的安全应满足：

a) 车辆必须支持基于非对称加密算法的数据签名/验签功能；

b) 车辆处理数据签名/验签算法处理时间不得超过 XX 毫秒；

c) 车辆必须支持自身的证书的新增、吊销及更新机制；

d) 车辆必须周期性的广播自身的证书（或摘要）信息；

e) 车辆必须对接收到的信息的发送方的证书有效性进行检验；

f) 车辆必须对接收到的信息进行完整性校验；

g) 车辆必须对接收到的信息内容中的时间和位置进行合理性检查；

h) 车辆在数据发送过程中必须采用随机 MAC 地址和设备 ID。

T/ITS 0035-2015

中国智能交通产业联盟标准

合作式智能运输系统 信息安全总体技术要求

T/ITS 0035-2015

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

2015 年 11 月第一版　2015 年 11 月第一次印刷