ICS 点击此处添加 ICS 号
点击此处添加中国标准文献分类号

中 华 人 民 共 和 国 国 家 标 准

GB/TXXXXX—XXXX

智能交通 数据安全服务

Intelligent transport - Data security service

（征求意见稿）

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。

（本稿完成日期：2017-7-31）

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准由全国智能运输系统标准化技术委员会(SAC/TC268)提出并归口。

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。

本标准起草单位：交通运输部公路科学研究院、北京中交国通智能交通系统技术有限公司、360企业安全集团、恒安嘉新(北京)科技股份公司、国家互联网应急中心、北京信息科技大学。

本标准主要起草人：王笑京、孟春雷、梅新明、周洲、孙婧、王立岩、武俊峰、宋向辉、王龑、郑新华、刘鸿伟、王永建、赵童、吴秋新。

智能交通 数据安全服务

1 范围

本标准规定了基于智能运输系统安全体系架构的安全支撑平台基本功能和系统构成，及安全支撑平台所提供的数据安全服务内容。

本标准适用于智能运输系统（包括合作式智能运输系统和车联网等应用）实现基于密码技术的数据安全服务。

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 20839-2007 智能运输系统 通用术语

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 22240-2008 信息安全技术 信息系统安全等级保护定级指南

GB/T 25069-2010 信息安全技术 术语

GM/T 0011-2012 可信计算 可信密码支撑平台功能与接口规范

GM/T 0034-2014 基于SM2密码算法的证书认证系统密码及其相关安全技术规范

GB/T XXXXX 交通运输 信息安全规范

3 术语和定义

下列术语和定义适用于本文件。为了便于使用，以下重复列出了GB/T 20839-2007和GB/T 25069-2010中的某些术语和定义。

3.1

智能运输系统 intelligent transport systems(ITS)

又称智能交通系统，是在较完善的交通基础设施之上，在先进的信息、通信、计算机、自动控制和系统集成等技术前提下，通过先进的交通信息采集与融合技术，交通对象交互以及智能化交通控制与管理等专有技术，加强载运工具载体和用户之间的联系，提高交通系统的运行效率，减少交通事故，降低环境污染，从而建立一个高效、便捷、安全、环保、舒适的综合交通运输体系。

[GB/T 20839-2007，定义2.1]

3.2

合作式智能运输系统 cooperative ITS

合作式智能运输系统是由载运装备单元、基础设施单元、数据传输网络、网络管理控制平台、业务管理平台、网关设备等部分共同组成的信息管理、控制、分发的系统，可以向交通运输管理者、业务提供者和使用者提供服务和应用的综合性信息系统。

3.3

车联网 internet of vehicles

车联网是以车内网、车际网和车载移动互联网为基础，按照约定的通信协议和数据交互标准，在车-X（X：车、路、行人及互联网等）之间（V2X），进行无线通讯和信息交换的大系统网络，是能够实现智能化交通管理、智能动态信息服务和车辆智能化控制的一体化网络，是物联网技术在交通系统领域的典型应用。

3.4

辅助驾驶 driving assistance

利用传感探测技术、自动控制技术和通信技术，通过车载装置和路边设施的智能探测以及车-车和车-路通信手段，为驾驶员提供信息服务与支持、紧急情况下的预警和控制干预支持等功能，提高驾驶员出行安全和效率。

[GB/T 20839-2007，定义7.2]

3.5

自动驾驶 automatic driving

利用传感探测技术、自动控制技术、通信技术和交通流理论等，通过车载装置和路边设施的智能探测、车-车和车-路通信手段，车辆自动操纵控制装置，在特定的道路上实现车辆自动运行。

[GB/T 20839-2007，定义7.3]

3.6

自动公路系统 automatic highway system

应用现代传感技术、通信技术、自动控制技术以及检测技术等装备车辆及公路系统，并通过车-路通信和车-车通信，达到自动控制车辆方向、速度、车间距等，从而使汽车以自由个体或编组形式自动形式在专用车道内。

[GB/T 20839-2007，定义7.19]

3.7

云计算 cloud computing

云计算是一种按使用量付费的模式，这种模式提供可用的、便捷的、按需的网络访问， 进入可配置的计算资源共享池（资源包括网络，服务器，存储，应用软件，服务），这些资源能够被快速提供，只需投入很少的管理工作，或与服务供应商进行很少的交互。

3.8

数据完整性 data integrity

数据没有遭受以未授权方式所作的更改或破坏的特性。

[GB/T 25069-2010，定义2.1.34]

3.9

保密性 confidentiality

使数据不泄露给未授权的个人、实体、进程，或不被其利用的特性。

[GB/T 25069-2010，定义2.1.34]

3.10

可用性 availability

已授权实体一旦需要就可访问和使用的数据和资源的特性。

[GB/T 25069-2010，定义2.1.34]

3.11

身份鉴别 identity authentication

是指在计算机及计算机网络系统中确认操作者身份的过程。

3.12

授权管理 authorization management

是指在计算机及计算机网络系统中对用户/设备访问和控制系统资源的权限进行管理的过程。

3.13

数据保护 data protection

采取管理或技术措施，防范未经授权访问数据。

[GB/T 25069-2010，定义2.1.34]

3.14

责任认定 accountability confirmation

是指在计算机及计算机网络系统中通过数字签名和安全审计等技术手段对用户/设备发生行为的事实进行确认的过程。

3.15

数字证书 digital certificate

由国家认可的，具有权威性、可信性和公正性的第三方证书认证机构（CA）进行数字签名的一个可信的数字化文件。

3.16

数字签名 digital signature

附加在数据单元上的数据，或是对数据单元所作的密码变换，这种数据或变换允许数据单元的接收者用以确认数据单元的来源和完整性，并保护数据防止被人（例如接收者）伪造或抵赖。

[GB/T 25069-2010，定义2.2.2.176]

4 缩略语

以下缩略语适用于本文件。

CA：认证机构（Certificate Authority）

DSRC：专用短程通讯（Dedicated Short Range Communications）

MAC：消息鉴别码（Message Authentication Code）

NFC：近场通信（Near Field Communication）

PDA：掌上电脑（Personal Digital Assistant）

PKI：公钥基础设施（Public Key Infrastructure）

V2I：车辆与基础设施间的信息交换（Vehicle-to-Infrastructure）

V2P：车辆与行人间的信息交换（Vehicle-to-Pedestrian）

V2V：车辆与车辆间的信息交换（Vehicle-to-Vehicle）

V2X：车辆与外界的信息交换（Vehicle-to-Everything）

5 安全支撑平台

5.1 平台概述

以密码技术为核心的安全支撑平台主要由证书认证系统、授权管理系统、密钥管理系统和安全管理系统共同构成，可为智能运输系统提供身份鉴别、授权管理、安全传输、数据保护、责任认定和安全管理六项数据安全服务。

根据应用需求不同，可构建与之相适应的安全信任模型。以车联网应用为例，基于PKI的安全信任模型可参考附录A。

5.2 系统构成

5.2.1 证书认证系统

证书认证系统为智能运输系统中各类交通参与实体提供身份注册、身份鉴别、身份隐私保护与身份管理功能，为授权管理、安全传输、数据保护和责任认定提供支撑。

证书认证系统一般性组成参见附录B。

5.2.2 授权管理系统

授权管理系统为智能运输系统中各类交通参与实体访问系统资源提供基本的访问控制并完成对系统资源高效、安全地配置。为授权管理服务提供支撑。

授权管理系统一般性组成参见附录C。

5.2.3 密钥管理系统

密钥管理系统为智能运输系统中各类交通参与实体提供密钥生产、分配、更新、销毁等密钥全生命周期服务。为身份鉴别、授权管理、数据保护、责任认定和安全管理服务提供密码技术支撑。

密钥管理系统一般性组成参见附录D。

5.2.4 安全管理系统

安全管理系统负责智能运输系统的安全管理，包括：安全策略制定、安全策略分发、安全审计、安全资源管理、安全防护、备份恢复、应急处理和灾难恢复等。为身份鉴别、授权管理、数据保护、责任认定和安全管理提供技术和管理支撑。

安全管理系统一般性组成参见附录E。

6 数据安全服务内容

6.1 身份鉴别

6.1.1 基本要求

智能运输系统应实现基于数字证书的身份鉴别功能，主要包括对设备/用户的身份进行标识和鉴别。

身份鉴别的参与实体可能包括：注册中心、CA中心、厂商。厂商为设备提供全球唯一的标识；注册中心根据用户/设备身份，为用户/设备颁发注册证书；CA中心认证证书的有效性后对用户/设备身份进行鉴别。基本要求包括标识要求和鉴别要求。

a) 标识要求包括：
   1) 应确保所标识用户在智能运输系统生存周期内的唯一性，并将用户标识与安全审计相关联；
   2) 对连接到智能运输系统的设备，应在将其接入到系统前先进行标识；
   3) 应对标识信息进行管理、维护，确保其不被非授权的访问、修改或删除。
b) 鉴别要求包括：
   1) 应采用数字证书技术实现设备/用户的身份鉴别，检测并防止使用伪造或复制的鉴别信息；
   2) 应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证信息系统中不存在重复用户身份信息，身份鉴别信息不易被冒用；
   3) 对连接到智能运输系统的设备，应在将其接入到系统前先进行鉴别，以防止设备的非法接入；
   4) 应提供鉴别失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

6.1.2 标识

智能运输系统中的标识包括设备标识和用户标识：

a) 对于系统中的设备（路侧单元、车载单元、移动终端）标识方式，见图 。

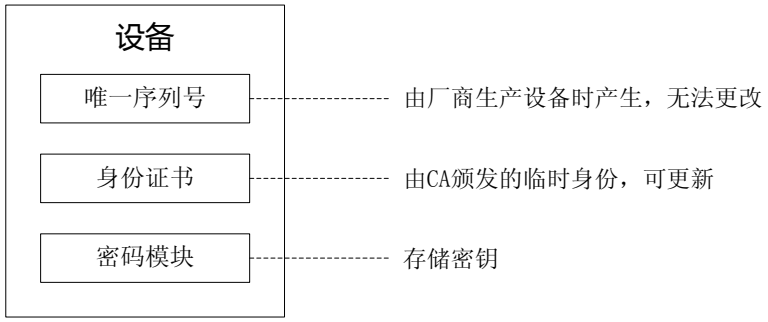


图 1 设备标识

设备的序列号为生产该设备的厂家在设备出厂时为其注册的唯一序列号，用于标识该设备。注册证书为其在系统中进行通信所需要申请的临时身份。密码模块用于存储通信所需密钥。

上述三部分由证书认证系统注册中心在设备实体申请身份时进行绑定。

b) 对于系统中的用户标识方式，见图 2。

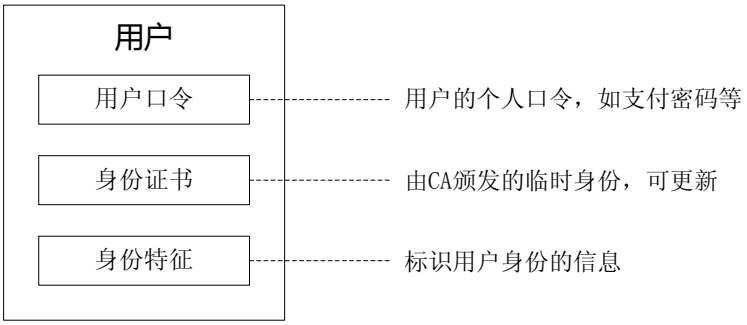


图 2 用户标识

用户口令为用户使用智能运输系统中的服务所需的用户个人口令。注册证书为其在系统中进行通信所需要申请的临时身份。身份特征，标识用户身份的信息或生物特征等。上述三部分由证书认证系统注册中心在用户实体申请身份时进行绑定。

6.1.3 鉴别

6.1.3.1.1 注册

证书认证系统注册中心负责接收设备/用户的注册请求，并判断该设备/用户提供的信息是否符合要求，其主要功能包括：

a) 信息录入：录入请求注册的设备/用户申请信息，包括签发证书所需要的信息，还包括用于验证身份的信息，这些信息存放在注册中心的数据库中，并将这些信息转换为符合系统特定格式的信息；

b) 信息审核： 提取请求注册的设备/用户申请信息，根据一定规则审核其真实身份；

c) 资格颁发： 当审核通过后，将证书签发所需要的信息提交给 CA 中心，将证书发放给设备/用户；

d) 关联绑定： 将设备/用户申请的临时身份信息与其身份关联进行绑定；

e) 安全管理： 对注册中心的登录进行安全访问控制，并对信息数据库进行管理和备份。

6.1.3.1.2 证书管理

6.1.3.1.3 证书颁发

设备/用户向注册中心提交请求并经过审核后，由 CA 中心颁发证书。

CA 中心最终确定是否接收设备/用户的证书申请，验证最终设备/用户的申请信息是否完整及合法，并向申请实体颁发或拒绝颁发证书。

6.1.3.1.4 证书更新

下列情况需要对证书进行更新：

a) 原证书过期；
b) 一些属性的改变；
c) 设备/用户要求发放新证书（如密钥泄露）；
d) CA 签名密钥更新。

6.1.3.1.5 证书撤销

下列情况需要对证书进行撤销：

a) 有条件（证书中信息修改等）要求证书的有效期在证书结束日期之前终止；
b) 要求设备/用户与私钥分离时（私钥可能以某种方式泄露）。

6.1.3.1.6 证书撤销列表

证书撤销列表标记了一系列不再被证书发布者所信任的证书列表，由CA中心签发，管理中心保管、维护与更新。

6.1.3.1.7 鉴别

基于证书的身份鉴别是指用户/设备在访问智能交通运输系统的过程中利用证书完成通信过程中的临时身份鉴别，以保证系统访问安全。

6.1.4 隐秘

证书认证系统管理中心的隐私保护功能负责对设备/用户的临时身份进行保护。在确认其身份真实性的前提下，通过后台支持技术来保证设备/用户的临时身份具有不可追踪性。

6.2 授权管理

6.2.1 基本要求

授权管理服务是对设备/用户访问受限资源的控制、管理。智能运输系统应在满足身份鉴别安全要求的基础上，基于授权证书实现授权管理服务。

已注册的设备/用户可向授权机构申请在注册机构和授权机构的授权范围内的访问权限。这些特权用授权证书来表示。当设备/用户申请授权证书时，应向授权机构出示其注册证书。当申请访问特定资源时，应向提供该资源的管理系统出示一个有效的授权证书。

授权关联基本要求包括：

a) 应由授权机构配置访问控制策略，并应依据安全策略控制设备/用户对资源的访问；
b) 授权管理的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；
c) 应具有对重要信息资源设置敏感标记的功能，并依据安全策略严格控制设备/用户对有敏感标记重要信息资源的操作。

6.2.2 获取授权证书

获取授权证书是设备/用户向一个或多个授权机构申请并且下载授权证书。包含：请求授权、验证证书和获得授权。

6.2.3 更新授权证书

授权证书颁发的数量应有限制，并且应该定期地进行更新。更新授权证书服务基本流程包含：请求更新、验证证书和更新授权。

6.2.4 发布授权状态

授权状态标识了设备/用户的授权信息，由授权中心保管、维护和更新。

6.2.5 更新本地授权状态存储

当设备/用户不能访问授权中心时，使用一个本地的授权状态库检验由其他设备/用户出示的授权信息。当设备/用户可以访问授权中心时，允许定时更新本地授权状态库。

6.3 安全传输

6.3.1 基本要求

智能运输系统在实现安全传输时应采用密码技术保障数据交换的机密性、完整性和可用性。当安全传输建立时，设备/用户之间应通过共有的身份鉴别与授权机制，以确保身份鉴别的有效性。

6.3.2 建立安全传输

允许两个实体建立一个单向的安全传输，以使一个实体可以安全的发送给另一个。允许两个实体建立一个双向的安全传输。

6.3.3 更新安全传输

允许两个已经分享一个安全传输的实体更新该安全传输的任何参数。

6.3.4 删除安全传输

允许两个实体终止一个已经建立起来的安全传输。

6.4 数据保护

6.4.1 基本要求

数据保护服务主要实现数据在存储、处理和交互过程中不因偶然或恶意的原因遭到破坏、更改和泄露，主要包括数据可用性、机密性、完整性保护几方面。

可采用校验值实现数据的完整性保护；可采用密码技术实现数据的保密性保护。

6.4.2 完整性保护

可采用附加消息鉴别码或数字签名的方式以保证数据传输的完整性。

6.4.3 保密性保护

应采用密码技术实现系统管理数据、鉴别信息和重要业务数据传输的保密性。

6.5 责任认定

6.5.1 基本要求

责任认定服务是对设备/用户在系统中操作行为的责任认定和证据管理。智能运输系统在实现责任认定时，应采用基于数字证书的数字签名功能。

应采用数字签名技术来确保发送数据的主体在数据交换期间能获得证明该数据被接收的证据，该证据可由该主体或第三方主体验证。

6.6 安全管理

6.6.1 基本要求

安全管理服务主要负责为智能运输系统中的身份管理、资源管理、审计管理、授权管理、密钥管理以及由它们支撑的安全服务提供安全策略管理、日志管理和核心系统的安全防御、备份恢复、应急响应和灾难恢复等功能。

6.6.2 安全策略管理

安全策略管理应根据系统规模设置相应管理组织，依据安全等级划分制定安全管理策略，设置系统正常安全运行机制，配置相应的安全管理人员。具体可参照GB/T 22239，GB/T 22240进行配置。

6.6.3 日志管理

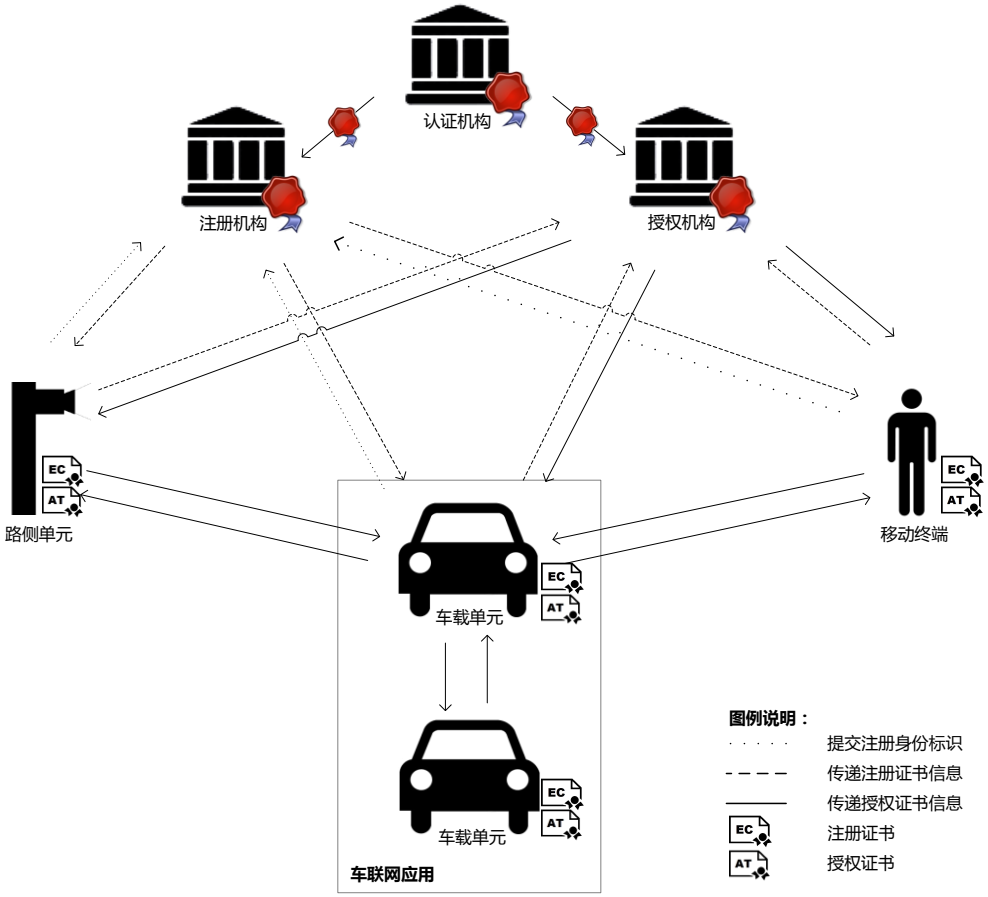
日志管理应记录智能运输系统运行中的重要操作，包括操作人员的信息、时间，对重要数据库的操作信息，系统运行成功或失败的信息等。

6.6.4 安全防御

安全防御应依据系统安全等级划分制定物理安全、网络安全、系统安全、主机安全和数据安全的安全防护。具体可参照GB/T 22239，GB/T 22240进行配置。

附 录 A
（资料性附录）
基于 PKI 的车联网安全信任模型

面向车联网应用的安全信任模型，见图A.1。



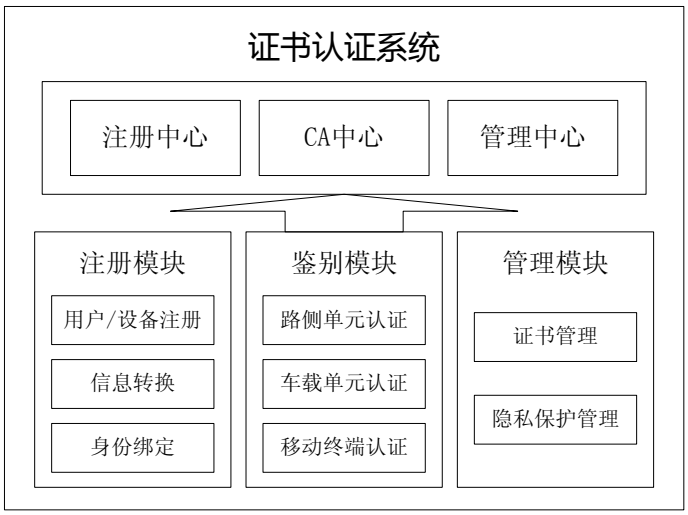
图A.1 基于 PKI 的车联网安全信任模型

面向车联网应用的公钥基础设施一般由认证机构、注册机构和授权机构共同构成，主要实现以下功能或操作：

a) 配置初始整体系统的安全参数。
b) 依据车辆、路侧设施或移动终端的特征标识，为其分配初始注册证书。
c) 依据车辆、路侧设施或移动终端的注册证书，为其颁发授权证书。
d) 将车辆、路侧设施或移动终端的授权证书散发给其他沟通方，使其可以验证签名的信息。
e) 撤销被滥用的注册证书或授权证书，并将CRL分发给其他沟通方。
f) 检测注册证书或授权证书被滥用的行为和具备异常行为的车辆、路侧设施或移动终端。

附 录 B
（资料性附录）
证书认证系统

证书认证系统一般性组成，见图B.1。



图B.1 证书认证系统构成

智能运输系统中的证书认证系统应由注册模块、鉴别模块和管理模块构成：

a）注册模块：实现对设备/用户的身份标识注册。需要认证的交通参与实体向注册中心提交相应信息，注册中心将其转换为符合系统特定格式的信息，完成证书申请；

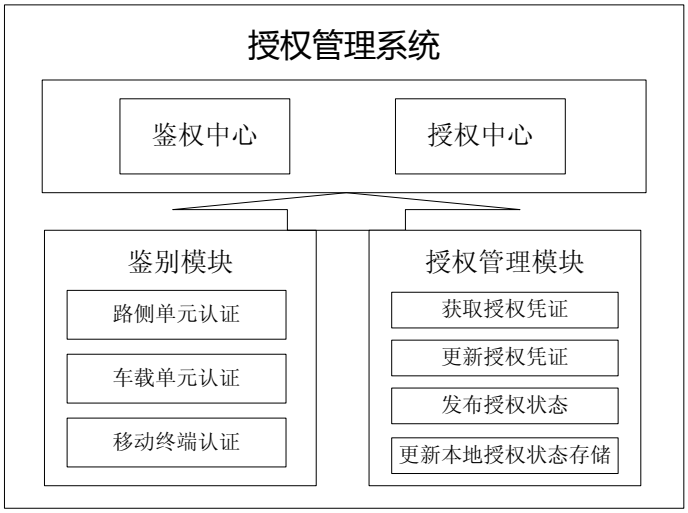
b）鉴别模块：实现对设备/用户的身份认证与识别；

c）管理模块：对生命周期内的证书进行全过程管理，为认证与授权提供依据。

认证系统应交由可信的第三方认证机构负责运营维护，系统中的数字证书格式应符合《GB/TXXXX-XXXX智能运输系统 信息安全 数字证书格式》要求。

附 录 C
（资料性附录）
授权管理系统

授权管理系统一般性组成，见图C.1。



图C.1 授权管理系统构成

智能运输系统中的授权系统应由鉴别模块和授权管理模块构成：

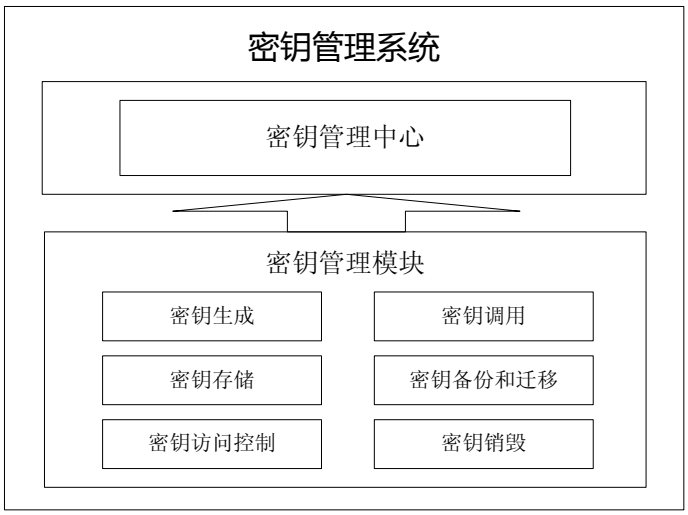
a) 鉴别模块：实现基础设施、车载端以及移动终端的身份的认证、识别；

b) 授权管理模块：维护凭证的全生命周期，为授权与鉴权提供依据。

授权系统应交由授权机构负责运营维护。

附 录 D
（资料性附录）
密钥管理系统

密钥管理系统一般性组成，见图D.1。



图D.1 密钥管理系统构成

智能运输系统中的密钥管理系统应具备密钥生成、密钥存储、访问控制、密钥调用、密钥备份迁移和密钥销毁功能。

根据密钥的使用范围，智能运输系统中的密钥可以分为四类：

a) 系统身份类密钥：与身份相关联的密钥。身份密钥用于对密码模块内部的信息进行数字签名，实现有身份的主体通信之间的身份识别；

b) 系统数据类密钥：与认证密钥配对构成双密钥（即双证书）。对通信实体间的数据进行加密，保证保密性；

c) 系统存储类密钥：加密密钥并存储密钥；

d) 用户类密钥：用于实现用户所需的密码功能，如下载娱乐服务、购物等过程中的机密性、完整性保护和身份认证等。

智能运输系统的密钥系统使用对称密码算法、非对称密码算法和数据摘要算法等三类算法实现有关密码服务各项功能，其中，对称密钥密码算法实现数据加/解密以及消息认证；非对称密钥密码算法实现签名/验证以及密钥交换；数据摘要算法实现待签名消息的摘要运算。

系统使用的密码算法要求如下：

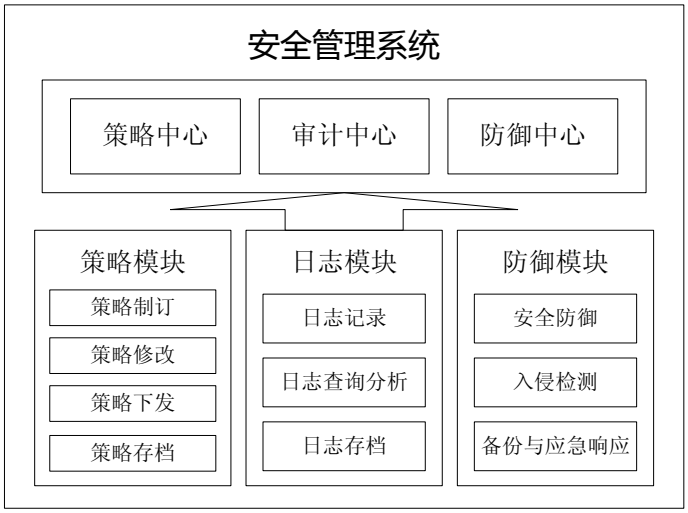
a) 对称密钥密码算法：采用国家密码主管部门批准使用的对称密码算法；

b) 非对称密钥密码算法：采用国家密码主管部门批准使用的非对称密钥密码算法；

c) 数据摘要算法：采用国家密码主管部门批准使用的数据摘要算法。数据摘要算法在实现待签名消息的摘要运算过程中，至少对部分数据要采取密码保护。

附 录 E
（资料性附录）
安全管理系统

安全管理系统一般性组成，见图E.1。



图D.2 管理系统构成

智能运输系统中的管理系统由策略模块、日志模块和防御管理模块相辅相成、相互协作，共同实现策略中心、审计中心和防御中心各项功能。

a) 策略模块主要负责为身份管理、资源管理、审计管理、授权管理、密钥管理以及由它们支撑的安全服务提供安全策略管理功能，包括：安全策略制定、安全策略下发、安全策略修改、安全策略存档管理等；

b) 日志模块主要负责为身份管理、资源管理、审计管理、授权管理、密钥管理以及由它们支撑的安全服务提供日志管理功能，包括：日志记录、日志查询与分析、日志存档管理等；

c) 系统自身安全防御模块主要负责智能运输系统的核心系统安全防御以及整体系统的入侵防御、备份恢复、系统冗余、应急响应和灾难恢复功能，包括：核心系统自身安全防御、入侵检测、备份与应急响应等。