ICS 03.220.20
R 85

# 中华人民共和国国家标准

GB/T 37373—2019

# 智能交通　数据安全服务

**Intelligent transport—Data security service**

2019-05-10 发布　　2019-12-01 实施

国家市场监督管理总局
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/TC 268)提出并归口。

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、中关村中交国通智能交通产业联盟、国家计算机网络与信息安全管理中心、北京信息科技大学、恒安嘉新(北京)科技股份公司、北京航空航天大学。

本标准主要起草人:梅新明、周洲、孙婧、王立岩、武俊峰、宋向辉、陈晓光、刘鸿伟、王永建、赵童、吴秋新、王云鹏、余贵珍。

# 智能交通　数据安全服务

## 1　范围

本标准规定了智能运输系统安全支撑平台和数据安全服务内容。

本标准适用于智能运输系统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 25069—2010　信息安全技术　术语

## 3　术语和定义

GB/T 20839—2007 和 GB/T 25069—2010 界定的以及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**

在较完善的交通基础设施上，将先进的科学技术(信息技术、计算机技术、数据通信技术、传感器技术、电子控制技术、自动控制理论、运筹学、人工智能等)有效地综合运用于交通运输、服务控制和车辆制造，加强车辆、道路、使用者三者之间的联系，从而形成的一种保障安全、提高效率、改善环境、节约能源的综合运输系统。

3.2

**合作式智能运输系统　cooperative ITS**

通过人、车、路信息交互，实现车辆和基础设施之间、车辆与车辆、车辆与人之间的智能协同与配合的一种智能运输系统。

3.3

**车联网　internet of vehicles**

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，在车与外界(车、路、行人及互联网等)之间进行无线通信和信息交换的大系统网络，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。

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的一种驾驶方式。

注：改写 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，在道路上实现车辆自动运行的一种驾驶方式。

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行驶在专用车道内的系统。

注：改写 GB/T 20839—2007，定义 7.19。

3.7

**云计算 cloud computing**

一种通过网络将可伸缩、弹性的共享物理和虚拟资源池以按需自服务的方式供应和管理的模式。

注：资源包括服务器、操作系统、网络、软件、应用和存储设备等。

[GB/T 32400—2015，定义 3.2.5]

3.8

**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 2.1.36]

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 2.1.1]

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 2.1.20]

3.11

**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。

[GB/T 20518—2006，定义 3.7]

3.12

**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)

PKI：公钥基础设施(Public Key Infrastructure)

## 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支撑平台。以车联网应用为例，基于 PKI 的安全支撑平台参见附录 A。

### 5.2 功能要求

安全支撑平台各系统功能要求如下：

a) 证书认证系统应具备注册功能、鉴别功能和管理功能，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服务。证书认证系统一般性功能描述参见附录 B。

b) 授权管理系统应具备鉴别功能和授权管理功能，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。授权管理系统一般性功能描述参见附录 C。

c) 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等密钥管理功能，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。密钥管理系统一般性功能描述参见附录 D。

d) 安全管理系统应具备策略功能、审计功能和防御功能，为智能运输系统提供安全管理服务，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。安全管理系统一般性功能描述参见附录 E。

## 6 数据安全服务内容

### 6.1 身份鉴别

#### 6.1.1 基本要求

身份鉴别主要包括对设备/用户的身份进行标识、注册和鉴别。

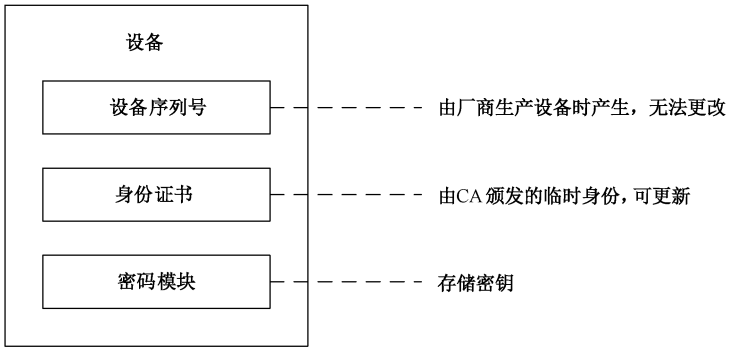
身份鉴别的参与实体一般包括：厂商、注册机构、CA 机构。厂商为设备提供全球唯一的标识；注册机构根据用户/设备的身份标识，为用户/设备颁发注册证书；CA 机构认证证书的有效性并对用户/设备身份进行鉴别。

#### 6.1.2 标识

设备和用户在接入到智能运输系统前应先进行标识，并确保其在生存周期内的唯一性。系统应对标识信息进行管理、维护，确保其不被非授权访问、修改或删除，并与安全审计相关联。

智能运输系统中的标识主要包括设备标识和用户标识：

a) 设备标识方式见图 1。




说明：

设备序列号——为生产厂家在设备出厂时为其注册的唯一序列号；

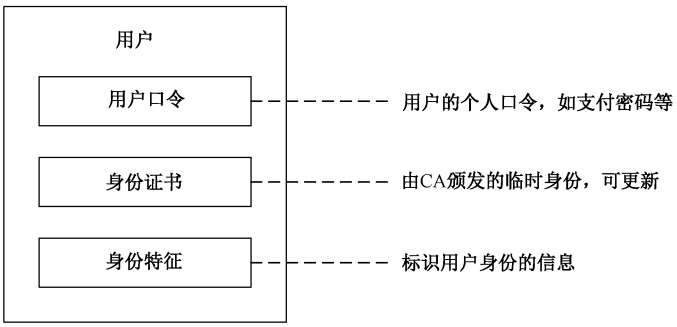
身份证书——为其在系统中进行通信所需要申请的临时身份；

密码模块——用于存储通信所需密钥。

**注**：上述三部分由注册机构在设备实体申请身份时进行绑定。

**图 1　设备标识**

b）　用户标识方式见图 2。




说明：

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；

身份证书——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。

**注**：上述三部分由注册机构在用户实体申请身份时进行绑定。

**图 2　用户标识**

### 6.1.3　注册

#### 6.1.3.1　注册申请

注册机构负责接收设备/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和用于验证身份的信息，并将这些信息转换为符合系统特定格式要求的信息后存放在注册机构数据库中；

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 机构，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。对注册机构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。

#### 6.1.3.2 证书管理

##### 6.1.3.2.1 概述

注册机构对注册申请进行审核后，由 CA 机构向设备/用户颁发证书，并对证书进行管理。

##### 6.1.3.2.2 证书颁发

设备/用户向注册机构提交请求并经过审核后，由 CA 机构确定是否接收设备/用户的证书申请，验证设备/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。

##### 6.1.3.2.3 证书更新

下列情况之一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。

##### 6.1.3.2.4 证书撤销

下列情况之一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)。

##### 6.1.3.2.5 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 机构签发，管理机构保管、维护与更新。

### 6.1.4 鉴别

智能交通运输系统应在通信过程中完成对用户/设备的临时身份鉴别，以保证系统访问安全，具体要求包括：

a) 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；

b) 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；

c) 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，以防设备的非法接入；

d) 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。

### 6.1.5 隐秘

智能交通运输系统应实现对设备/用户的隐私保护功能。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

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。

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，应向拥有该资源的管理系统提供一个有效的授权证书。

授权管理基本要求包括：

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

设备/用户向一个或多个授权机构申请并且下载授权证书。获取授权证书基本流程包含：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，由授权机构保管、维护和更新。

#### 6.2.5 更新本地授权状态存储

当设备/用户不能访问授权机构时，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/用户可以访问授权机构时，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保密性、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

两个实体之间可建立单向安全传输，也可建立双向安全传输。

#### 6.3.3 更新安全传输

两个已经建立安全传输的实体可更新该安全传输的任何参数。

#### 6.3.4 删除安全传输

两个已经建立安全传输的实体可删除该连接。

### 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，主要包括数据完整性、保密性、可用性保护三方面。

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方式实现数据传输的完整性保护。

#### 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。

#### 6.4.4 可用性保护

应采用密码技术保障授权用户或实体在需要时可以使用和访问数据或资源。

### 6.5 责任认定

智能运输系统应对设备/用户在系统中操作行为进行责任认定和证据管理，一般采用基于数字证书的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

智能运输系统应为身份管理、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、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安全管理功能，具体可按照 GB/T 22239—2008 中 7.2 进行配置。

# 附 录 A
（资料性附录）
## 基于 PKI 的车联网安全支撑平台

基于 PKI 的车联网安全支撑平台由密钥管理系统、证书认证系统、授权管理系统和安全管理系统四部分构成：

a） 密钥管理系统：提供密钥生产、分配、更新、销毁等密钥全生命周期服务；

b） 证书认证系统：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） 授权管理系统：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） 安全管理系统：负责安全策略制定、安全策略分发、安全审计等功能。

基于 PKI 的车联网安全支撑平台见图 A.1。

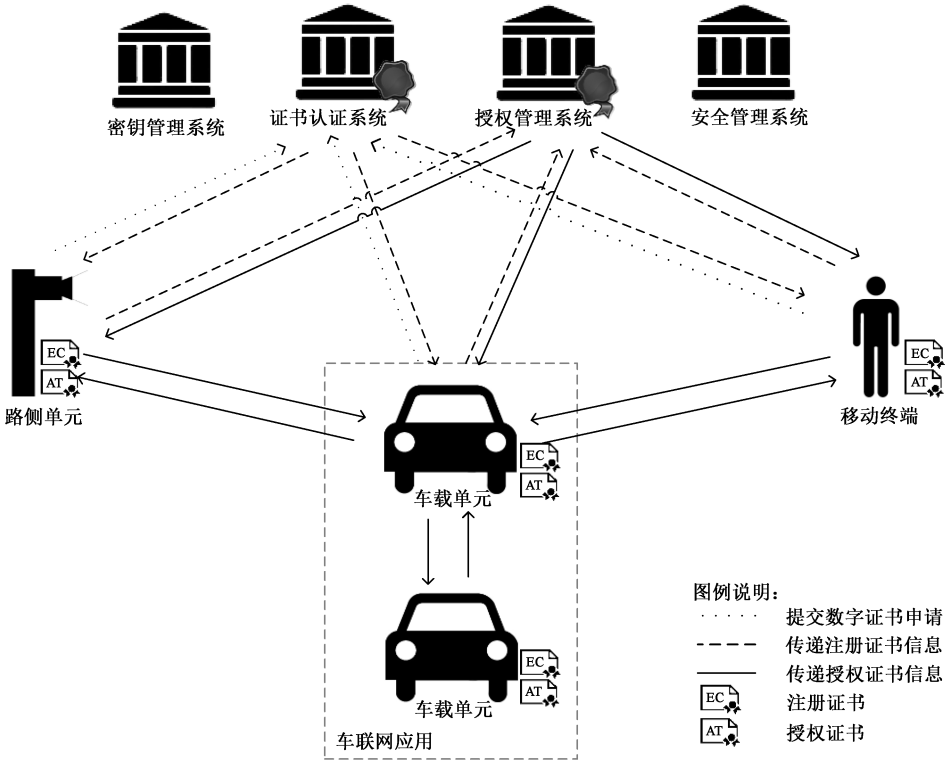



图 A.1 基于 PKI 的车联网安全支撑平台

# 附 录 B
（资料性附录）
证书认证系统

证书认证系统应具备注册功能、鉴别功能和管理功能：

a） 注册功能：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机构提交相应信息，注册机构将其转换为符合系统特定格式的信息，完成证书申请；

b） 鉴别功能：实现对设备/用户的身份认证与识别；

c） 管理功能：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。

证书认证系统一般交由专业认证机构负责运营维护，系统中的数字证书格式参见 GB/T 37376—2019。

证书认证系统一般性功能组成见图 B.1。

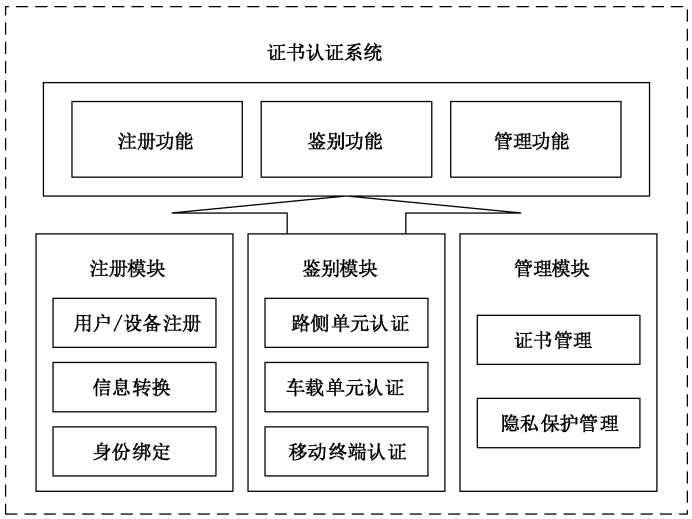



图 B.1 证书认证系统一般性组成

# 附 录 C
（资料性附录）
# 授权管理系统

授权系统应具备鉴别功能和授权管理功能：

a） 鉴别功能：实现基础设施、车载端以及移动终端的身份的认证、识别；

b） 授权管理功能：维护凭证的全生命周期，为授权与鉴权提供依据。

授权系统一般交由授权机构负责运营维护。

授权管理系统的一般性功能组成见图 C.1。

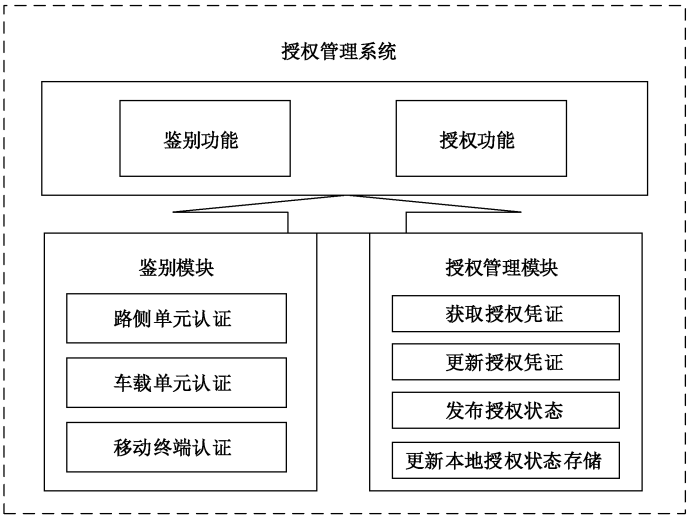



图 C.1 授权管理系统一般性组成

# 附 录 D
（资料性附录）
密钥管理系统

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等密钥管理功能。

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。

密钥管理系统一般性功能组成见图 D.1。

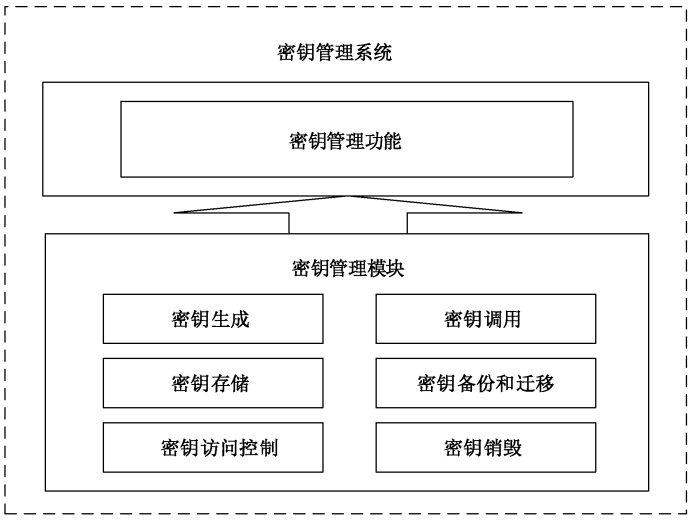



图 D.1 密钥管理系统一般性组成

# 附 录 E
（资料性附录）
安全管理系统

安全管理系统应具备策略功能、审计功能和防御功能：

a） 策略功能：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） 日志功能：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） 防御功能：主要负责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。

安全管理系统一般性功能组成见图 E.1。

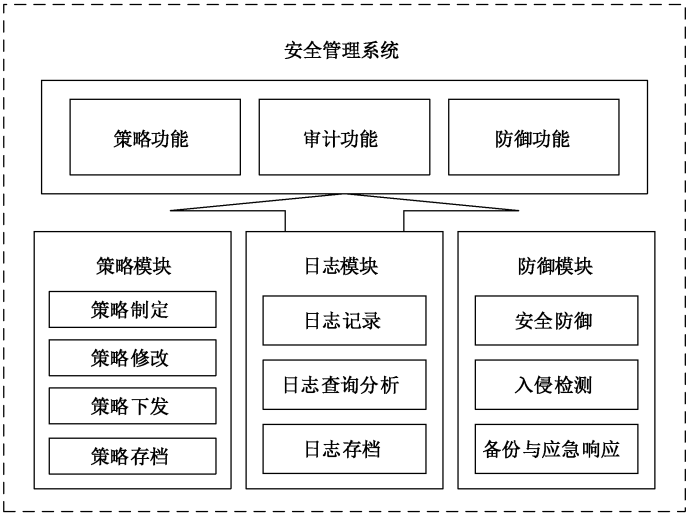



图 E.1 管理系统构成

# 参 考 文 献

[1] GM/T 0011 可信计算 可信密码支撑平台功能与接口规范
[2] GM/T 0034 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
[3] GB/T 22240 信息安全技术 信息系统安全等级保护定级指南
[4] GB/T 37376—2019 交通运输 数字证书格式