

ICS 35.240.60
CCS A



中华人民共和国国家标准

GB/T XXXXX—XXXX/ISO 37163:2020

智慧城市基础设施 智慧交通中城市停车位 分配指南

Smart community infrastructure — Smart transportation for parking lot allocation in
cities

(征求意见稿)

(ISO 37163:2020, Smart community infrastructure — Smart transportation for
parking lot allocation in cities, MOD)

2023年11月17日

XXXX - XX - XX 发布

XXXX - XX - XX 实施

国家市场监督管理总局
国家标准化管理委员会

发布

目 次

前 言	iii
引 言	iv
1 范围.....	1
2 规范性引用.....	1
3 术语和定义.....	1
4 智慧交通中停车位分配系统的概念.....	1
4.1 概述.....	1
4.2 适用的城市问题和预期优势.....	2
5 规划实施智慧交通中停车位分配系统.....	2
6 智慧交通中停车位分配系统的应用和运营.....	3
6.1 目标.....	3
6.2 服务车辆.....	3
6.3 采用智慧交通中停车位分配系统的流程.....	3
6.3.1 概述.....	3
6.3.2 收集的信息要素.....	3
6.3.3 信息收集.....	4
6.3.4 数据传输.....	4
6.3.5 信息发布.....	4
6.3.6 停车位分配.....	5
6.3.7 停车收费.....	5
6.3.8 提供有利于停车位分配管理的信息.....	6
7 数据共享与管理.....	6
8 智慧交通中停车位分配系统的数据安全管理.....	6
8.1 概述.....	6
8.2 隐私信息保护.....	7
9 智慧交通中停车位分配系统的质量维护.....	7
9.1 概述.....	7
9.2 需监控的参数.....	7
9.3 智慧交通中停车位分配系统的优化.....	8
附录 A (资料性) 当前主要密钥系统的关键性能指标比较.....	9
参考文献	10

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。

本文件做了下列最小限度的编辑性改动：

- a) 删除了3.1节的注1；
- b) 删除了3.1节的注2。

本文件主要技术变化如下：

- a) 在范围以及停车位分配系统的概念概述部分、停车位分配系统的流程概述、停车位分配系统的维护概述中，删除对ITU-T. Y. 4456[6]的引用（见第1章、第4章4.1、第6章6.3.1、第9章9.1）；
- b) 更改了关于停车位分配系统确保高性能的基本要求中，关于数据安全、隐私保护、数据通信能力的具体描述（见第4章4.1）；
- c) 增加了停车位分配系统额外效益中关于环保、可持续发展的描述（见第4章4.1）；
- d) 删除了关于停车位分配系统的通信和数据共享的目标点对点通信和可追溯性通信要求条款（见第4章4.1）；
- e) 增加了停车位分配系统的架构图（见第6章6.1）；
- f) 修改了数据传输流程中通讯要求中对停车场设备和驾驶员之间的通讯的要求（见第6章6.3.4）；
- g) 增加了停车收费要求中对车辆标识设备、控制和感应设备、车辆识别设备、位置识别设备、自组网络设备以及应对突发灾害和特殊场景能力的要求（见第6章6.3.7）；
- h) 增加了对数据共享与管理的具体要求，并明确了数据共享包括停车分配系统内的共享和停车分配系统与外部系统的共享（见第7章）；
- i) 删除了停车位分配系统安全技术方案中对于公钥密钥算法使用过程的具体描述（见第8章8.1）；
- j) 增加了停车位分配系统对公钥密钥系统关于技术自主可控、分类分级管理、终端安全保护、大规模使用、业务流程、双离线交易和低成本的要求（见第8章8.1）；
- k) 增加了附录A（资料性）：当前主要密钥系统的关键性能指标比较。

本文件由全国城市可持续发展标准化技术委员会（SAC/TC 567）提出并归口。

本文件起草单位：。

本文件主要起草人：。

引 言

本文件旨在不大幅增加车位资源建设运营投入情况下解决城市停车难问题。本文件提供了基于安全、高效、精准且低成本数字技术的停车位分配系统的实施指南，从而充分利用现有停车场与车位资源，帮助驾驶员快速找到合适的停车位，并使其享受智能便捷的定位、停车、缴费等全流程数字化服务。

当前，我国城市人均汽车拥有量不断攀升，停车难问题日益严重。对于驾驶员而言，停车难问题不但会导致时间的浪费，还可能导致情绪焦躁，产生不良影响，如加剧乱停乱放、交通拥堵等现象，严重影响市民的正常生产生活，还带来了巨大的城市治理成本。除此之外，停车难问题还可能间接导致更多的污染物、颗粒物（PMs）和温室气体排放到大气中，以及交通事故增多和噪音污染问题等。

本文件通过优化停车位分配来为驾驶员提供更好停车服务与体验，促进城市管理降本增效，将所有停车位进行最优配置并分配给有停车需求的驾驶员，从而大幅提升停车场的利用效率与服务效率，并帮助城市治理者提升城市治理能力和效果。

本文件有助于：

——利用安全高效低成本的基于可信数字身份的数据共享与交换技术，实现停车场位置的合理分配，解决停车难问题，增强城市居民在数字技术进步中的获得感；

——缓解城市道路交通的拥堵，降低交通事故发生率，并帮助解决环境污染、噪音污染等其他城市问题，促进城市绿色发展。

智慧城市基础设施 智慧交通中城市停车位分配指南

1 范围

本文件规定了为驾驶员提供智慧交通中停车位分配系统的实施和组织程序。它适用于城市，特别是那些停车场短缺或利用率低下的城市。这种智慧交通中停车位分配系统旨在为驾驶员快速找到可用的停车位、并获得安全高效精准的停车相关服务提供解决方案。它还旨在解决其他城市问题，例如交通事故、拥堵和能源消耗。

2 规范性引用

本文件无规范参考。

3 术语和定义

下列术语和定义适用于本文件。

3.1

停车位 parking lot 或者 car park

能够停放允许在公共道路上行驶的车辆的地方。¹

3.2

停车位分配 parking lot allocation

基于驾驶员的要求或停车偏好，找到与当前或预期可用的停车场位置之间的最优匹配，并向驾驶员建议停车场（3.1）的车位。

注 1：驾驶员的要求包括从当前位置出发的到达路线、首选的停车地点、首选的开始停车的时间、停车时长、要停放的车辆数量和车辆特征、停车费用限制及支付方式。

3.3

停车位分配系统 parking lot allocation system

通过信息交换和共享来实现停车位分配（3.2），这些信息包括停车场位置、停车时间、停车位导航、停车费支付信息和相关服务信息等。

4 智慧交通中停车位分配系统的概念

4.1 概述

本条描述了智慧交通中停车位分配系统所需的通用准则。为了解决城市中驾驶员难以找到可用停车场的问题，宜组织实施智慧交通中停车位分配系统，为驾驶员快速找到可用车位提供方案，并根据他们的要求和偏好预约停车位。可以通过提高城市停车场的可获得性来实现这种预约服务，提升可获得性宜采用：

- a) 为市民和城市游客提供数量更多的停车位；
- b) 为市民和城市游客提供更高效的停车服务及相关服务。

为确保高性能，智慧交通中停车位分配系统具有如下特点：

¹ 根据 GB/T 51149-2016 城市停车规划规范 2.0.2 对停车位的定义“为停放车辆而划分的停车空间或机械停车设备中停放车辆的部位。由车辆本身的尺寸加四周必需的空间组成。”

- a) 保护驾驶员和停车场所有者的隐私，保障停车费缴付和各类敏感数据、应用与交易数据端-边-云全环节全流程安全，避免隐私和敏感数据泄露或被篡改等而导致的损害与损失；
- b) 智能终端设备之间具有点对点、安全可信的数据通信能力、并在点对点安全可信通信基础上实现可信的双离线交易，降低整个系统的组织、运营和维护成本，同时保持高安全性与高扩展性。

由于智慧交通中停车位分配系统可以减少驾驶员寻找可用停车位及完成停车流程的时间，因此智慧交通中停车位分配系统可以提升城市停车位利用率，从而间接实现以下额外效益：

- a) 使城市可以容纳更多的游客；
- b) 可以为城市创建和引进更多商业机会；
- c) 减少车辆碰撞和交通事故；
- d) 缓解交通拥堵；
- e) 缓解因道路拥堵导致的驾驶员不适感和进一步导致的附近居民的不适感；

注：由于操作单调，缓慢驾驶会使驾驶员感到无聊，同时低频噪音和振动刺激居民。

- f) 降低城市在驾车出行方面的建设成本和运营成本，降低能耗和污染，促进碳中和、碳达峰计划落地。
- g) 停车定价策略和实时价格之间的协同作用，可以减少司机寻找车位和完成停车的时间。

在一个城市的不同地点，有各种各样的车辆开往各自的目的地。建立安全高效精准且低成本数字技术支持的停车位分配服务平台是成功组织停车位分配服务的关键。信息需要在系统注册驾驶员、停车场所有者以及停车位分配服务平台之间共享。停车位分配服务平台宜根据驾驶员的需求或偏好与停车场的状况相匹配来分配停车位，这些停车场是在驾驶员要求或偏好的时间段可用的停车场。

智慧交通中停车位分配系统宜实现以下目标：

- a) 减少业务流程的时延（例如，在保证结果真实、可信前提下减少用户识别认证的处理步骤）；
- b) 提供充足的信息用于停车位的选择；
- c) 便于服务管理。

新能源停车场旨在将清洁的新能源电能与电动交通的应用相结合。新能源电池板可提供遮阳作用，并为停放的电动汽车充电。在车辆与电网的对接中，车辆也可以为电网提供辅助服务和支持。新能源停车场应满足：

- a) 提供环境和技术层面的有益效果；
- b) 减少电网所需的太阳能，并使收益最大化；
- c) 鼓励停车场设置新能源停车位。

4.2 适用的城市问题和预期优势

本文件中描述的智慧交通中停车位分配系统准则，为解决驾驶员停车难问题提供方案。如4.1所述，智慧交通中停车位分配系统的引入除了解决这一问题外，还将带来其他优势，比如减少在公共场所随意停车，减少停车场占用的土地资源。

5 规划实施智慧交通中停车位分配系统

为正确实施并按照计划顺利运营智慧交通中停车位分配系统，应在实施前确认以下参数：

- a) 目标城市或区域的交通模式；
- b) 目标城市或地区的交通量；
- c) 目标城市或区域内公共道路的交通容量；
- d) 现有停车场数量；
- e) 现有停车场的位置；
- f) 现有停车场的面积或容量；
- g) 规划停车场的数量；
- h) 规划停车场的位置；
- i) 规划停车场的容量；
- j) 停车场允许的重量限制；

- k) 停车场允许的尺寸限制（如间距）；
- l) 停车场可用的付款方式；
- m) 城市中使用的新型车辆的信息。

6 智慧交通中停车位分配系统的应用和运营

6.1 目标

如4.2所述，智慧交通中停车位分配系统，可以为城市内司机寻找空闲停车位提供直接帮助。智慧交通中停车位分配系统应按照以下6.3要求具体实施。

停车位分配系统的架构如图1所示：

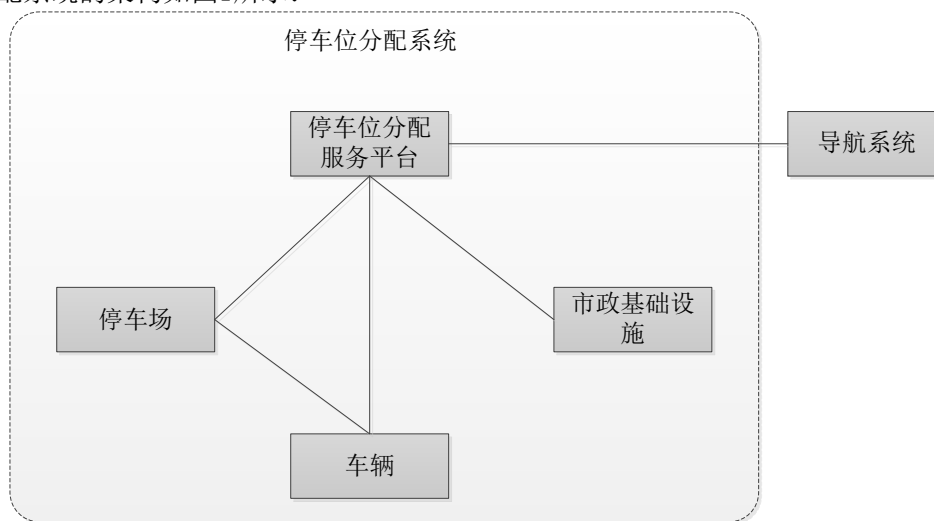


图1 停车位分配系统架构图

6.2 服务车辆

所有能停放在城市停车场的车辆。

6.3 采用智慧交通中停车位分配系统的流程

6.3.1 概述

一个城市在部署智慧交通中停车位分配系统时应遵循6.3.2至6.3.8描述的程序。

6.3.2 收集的信息要素

智慧交通中停车位分配系统向驾驶员分配停车位时，停车位分配服务平台应收集如下信息要素：

- a) 停车场
 - 1) 位置；
 - 2) 组成或结构（如地面、地下、建筑物内部、桥梁上、公共道路上）；
 - 3) 尺寸或容量（即尺寸或容量足以容纳标准私人车辆）；
 - 4) 对于共享车位，共享出来供他人使用的时间段（起始共享时间，结束共享时间）；
 - 5) 停车服务时间范围（例如，仅在白天，包含夜间，过夜）；
 - 6) 对于共享车位，共享的方式（例如，一次性共享，固定时间段的长期共享等）；
 - 7) 所有权（例如公共、共享）；

- 8) 便利设施（如带屋顶车位、代客泊车服务、充电、加油、洗车服务）；
- 9) 智慧交通服务服务区域的地图；
- 10) 停车费（如金额、折扣或合作计划）。
- b) 司机
 - 1) 性别；
 - 2) 年龄；
 - 3) 特殊情况（如残疾、带有婴儿或幼儿）；
 - 4) 当前位置；
 - 5) 目的地；
 - 6) 车辆特性（例如标准私人车辆，车辆的长度、宽度、高度和重量）；
 - 7) 要求或预期停车时间（例如15分钟、30分钟、1小时、半天、一整天、一周、一个月、半年、一年）；
 - 8) 首选支付程序[例如仅现金、信用卡、数字支付（d-payment）、银行转账、在线或离线支付交易）。
- c) 其他
 - 1) 在前往停车场的路上以及停车场当地的当前天气状况（例如：日照、云、雨、雪、风速和风向、湿度、能见度、特定天气条件）。

6.3.3 信息收集

为收集6.3.2中指定的信息，应安装和运行以下仪器和设备：

- a) 停车场的车辆传感器（例如，检查某辆车是否在停车位，停车位是否空置或占用）；
- b) 停车场安全监控；
- c) 交通拥堵监测器（例如，在前往停车场的路上和停车场周围区域）；
- d) 大气条件传感器（例如，检查环境温度、湿度）；
- e) 天气监测器（例如，检查降雨量、降雪量、风速和风向、能见度）；
- f) 用于收集和处理数据的软件（如数据收集、数据传输、数据处理、停车收费、停车费收集）；
- g) 应用程序（如提供给司机、停车场业主、交通部门的相关和附加服务）。

6.3.4 数据传输

为了将6.3.2和6.3.3中列出的数据传输到停车场分配系统服务平台、驾驶员和停车场所有者，应通过以下方式组织通信：

- a) 停车场业主和停车场分配系统之间的通讯：
 - 1) 智能手机；
 - 2) 手机应用；
 - 3) 安全网关（如身份认证、数据加密、访问控制和限制）；
 - 4) 互联网。
- b) 驾驶员和停车场分配系统之间的通讯（除a中指定的要求和功能外）：
 - 1) 使用标签进行识别和跟踪（例如无线电或超高频识别）。
- c) 停车场设备与驾驶员之间的通讯：
 - 1) 支持点到点通讯（如通过自组网、近场通信进行通讯）。

6.3.5 信息发布

为了帮助驾驶员选择出最符合他们的需求和偏好的停车位，如停放哪里、什么时候停车、以及停放多长时间，停车位分配服务器应向驾驶员提供以下信息：

- a) 位置；
- b) 可用时间范围（例如从什么时间开始到什么时间结束）；

- c) 允许停车时间（如30分钟、1小时、半天、一天、一周、一个月、半年、一年）；
- d) 进场路线；
- e) 从驾驶员当前位置开车到达停车场的的预计时间；
- f) 停车费（如每小时、每天、每周、每月或每年的价格）；
- g) 电动汽车充电设施的可用性；
- h) 可用的日期和时间（例如工作日、周末、节假日、白天或夜间）；
- i) 途中或附近的道路状况（例如交通拥堵、天气状况、事故、道路施工）；
- j) 停车费支付方式（如现金、信用卡、数字化支付、银行转账、线上线下支付）；
- k) 对司机有帮助的附加信息（例如附近的商店、餐馆、公共浴室、加油站）。

6.3.6 停车位分配

为了成功地分配停车位，停车位分配服务平台将对驾驶员们的请求或偏好和停车场信息进行比较，特别是关于以下列出的信息。并保留最佳匹配结果，直到停车位预订信息被确认或超时。

- a) 驾驶员请求和偏好
 - 1) 当前地点；
 - 2) 首选停车地点；
 - 3) 开始停车的首选时间；
 - 4) 停车时间（例如多少分钟、多少小时或多少天）；
 - 5) 待停放车辆的数量（例如，仅一辆车，多辆车）；
 - 6) 车辆特性（如标准个人用车、标准尺寸商务车）；
 - 7) 停车费支付方式（如数字钱包信用卡、银行转账、积分支付等）。
- b) 停车场服务
 - 1) 位置；
 - 2) 可用停车位数量；
 - 3) 可用停车时间范围（例如从什么时间到什么时间）；
 - 4) 对于共享车位，共享的方式（例如，一次性共享，固定时间段长期共享等）；
 - 5) 停车场的附加服务（如充电器、加油站、浴室、便利店）；
 - 6) 停车场周围的可用设施（如商店、餐厅、银行和自动取款机、医院和诊所、车站、公共汽车站、渡轮码头、机场、酒店、邮局、警察局）；
 - 7) 停车场安全保证（如保安、电视监视器）；
 - 8) 停车费；
 - 9) 停车费支付方式（如数字钱包、信用卡、银行转账、积分支付等）；
 - 10) 电动汽车充电设施的可用性。
- c) 指定用途
 - 1) 指定为“禁止停车或停车”的专用空间和车道标志，以便紧急车辆（如消防设备、救援车辆、警车、救护车）进入；
 - 2) 为残疾人提供专用停车位标识。

6.3.7 停车收费

为了便利驾驶员停车及缴费，车辆上应该安装车辆标识设备，包括：

- a) 身份标识芯片；
- b) 通信芯片，如支持蓝牙、RFID、自组网、北斗卫星定位等的芯片。

停车场应安装和操作下列仪器设备：

- a) 停车控制和感应设备，如栅栏门、地锁、车位上的车辆感应设备等；
- b) 车辆识别设备，例如摄像头、蓝牙或者RFID识读设备等；
- c) 位置识别设备，例如北斗卫星定位辅助设备；
- d) 自组织网络设备；

- e) 指示牌或显示器，以告知司机预计或者确定的停车费数额；
- f) 通知驾驶员允许停车的剩余时间的标志牌或显示器；
- g) 指示停车费缴付方式的指示牌或显示器；
- h) 收取停车费的工具（如数字钱包、电子或数字收款设备、收据打印机）。
- i) 考虑突发灾害等特殊情况，以及地下车库可能没有网络覆盖等情况，以及其他任何可能的情况，驾驶员终端设备和停车场设备之间应支持可信离线认证与安全交易。

6.3.8 提供有利于停车位分配管理的信息

为妥善组织和管理停车位分配系统，停车场应提供以下信息：

- a) 非法停放车辆信息（如超期停车、超限停车、偷逃停车费等）；
- b) 未在停车位分配服务系统登记的车辆信息；
- c) 所欠停车费；
- d) 经常使用的用户（例如折扣、下一次预订的优先权）；
- e) 仪器设备现状；
- f) 仪器设备维护状态及记录。

7 数据共享与管理

为了妥善管理和运行停车位分配系统，在第5章、第6.3.2节和第6.3.8节中的数据，需要安全保存并正确处理；第6.3.3节和第6.3.5节的数据需要被安全地传输。同时，为了促进智慧交通和城市建设，停车场分配系统还应与外部关联系统之间建立合适的安全数据共享和交换体系。数据交换与共享平台以及网络基于GB/T 43245-2023《智慧城市基础设施 数据交换与共享指南》进行。

停车场分配系统内部不同模块或子系统之间的数据共享和管理，以及停车场分配系统与外部系统之间的数据共享和管理均宜满足以下要求：

- a) 高安全性，在数据共享过程中应采取双向认证、加密和完整性保护等方法，有效防范共享和管理中数据被窃取、伪造、非法篡改等安全问题；
- b) 实时性，具备高并发处理能力，并能够快速完成海量数据的共享和管理；
- c) 基于唯一可信数字身份标识，对数据共享与管理的主体和对象实现精准管理，保证数据共享过程中人、物、数据的身份均安全可信、可以追溯；
- d) 精细权限管理模式，通过唯一可信数字身份标识对数据共享与管理的主体进行子域划分管理，明确不同子域的权限，防止数据共享用于超出权限要求的范围；
- e) 明确数据的权属关系，通过多层次、多维度的关联关系全面反映人、物、数据之间的多种权属与关联关系，保证数据资产在共享和流通过程中可以安全、可靠地确权，防止价值贬损；
- f) 可获得性，对于地震、洪灾、无网络覆盖等场景，或其他任何需要的地方，应支持基于点对点通信模式的可信数据共享，以保证业务的可获得性；
- g) 审计性，对数据共享制定安全审计策略和审计日志管理操作规范，记录数据共享活动日志，为数据共享相关安全事件的处置、应急响应和事后调查提供证据支撑。

8 智慧交通中停车位分配系统的数据安全管理

8.1 概述

依托数字科技建立的智慧交通中停车位分配系统，应保证数据收集的真实性及使用、交换和共享过程中的安全性，防止未经授权的非法访问和利用，尤其应防止以下攻击或操作造成的安全风险问题：

- a) 信息窃取；
- b) 冒充；
- c) 篡改；
- d) 信息否认；

e) 隐私泄露。

为满足上述数据安全需求，应使用公钥体制及相关底层密钥技术。智慧交通中停车位分配系统采用的公钥密钥系统应该满足如下要求：

- a) 底层基础设施安全技术应符合自主可控、数字安全的国家战略方向，宜采用相关国家标准推荐的安全技术；
- b) 满足数据分领域、分等级安全管理需要，并保证数据在端-边-云全环节及采集、传输、交换、存储等全流程中的安全；
- c) 支持各类移动智能终端、物联网智能设备进行采集、处理、存储数据的安全保护；
- d) 支持大规模并发使用，允许海量终端接入停车位分配系统，且在业务进行前都需要进行双向可信认证，都需要加密、完整性保护和不可抵赖性保护；
- e) 业务时延短；
- f) 支持双离线状态下的安全交易，对于发生地震、洪灾等灾害导致或地下停车场等等网络难以覆盖的情况，能满足双向认证、签名与验签等离线操作需要，以保证业务的正常进行；
- g) 低成本：在达成上述各类各项安全管理要求与目标的同时，大幅降低整个安全方案的实施成本及硬件投入，以符合利用数字技术促进智慧交通发展的社会意义及经济价值。

为满足上述数据安全需求，宜采用GB/T 36625.3-2021《智慧城市 数据融合 第3部分：数据采集规范》第9.2节中推荐使用的CCKS无中心化标识认证与密钥体系。

注：当前主要密钥系统的关键性能指标比较参见附录A。

8.2 隐私信息保护

为了防止个人隐私泄露，只有经过授权的安全组织才能根据为保护用户隐私而制定的措施访问数据库。

9 智慧交通中停车位分配系统的质量维护

9.1 概述

为保持智慧交通中停车位分配系统的预期性能，并确认其有效性，宜定期观察9.2中的参数。

如上文和ISO 37154:2017第7条所述，已实施并正在运营智慧交通中停车位分配系统的条件可能会发生变化。因此，要成功地运营智慧交通中停车位分配系统，解决目标城市问题并长期保持运营绩效，智慧交通中停车位分配系统的质量维护是必不可少的。

9.2 需监控的参数

用于比较智慧交通中停车位分配系统性能的参数如下。需要采用合适的方式监控如下项目：

- a) 在目标城市或地区从寻找车位到完成停车的平均时间；
- b) 目标城市或区域内可用停车位的绝对数量；
- c) 目标城市或地区在各个时间段内可用的停车位数量（如每小时、日、周、月、年）；
- d) 目标城市或区域的停车场的可获得性；

注：为供参考，可对下列参数进行监控，以显示如4.1所述的通过智慧交通中停车位分配系统间接获得的优势。

- e) 目标城市或地区的外来游客数量；
- f) 目标城市或地区的经济指标（如目标城市或地区单位时间的燃料消耗成本）；
- g) 目标城市或区域内发生的车辆碰撞和交通事故数量；
- h) 目标城市或区域的交通拥堵指标；
- i) GB/T 36749-2018和ISO 37122:2019中指定的公民便利性指标；
- j) 单位时间（小时、日、周、月、年）内目标区域内智慧交通提供的停车位数量与登记停车请求的比例。

9.3 智慧交通中停车位分配系统的优化

对于9.2中指定监控的参数值，如果在实施智慧交通中停车位分配系统的前后没有变化，可改变6.3所述的智慧交通中停车位分配系统的实施条件。为了对智慧交通中停车位分配系统进行优化，需考虑实施区域的特殊本地条件和异常情况。监测系统运营运行状况，及时修正运营中的智慧交通中停车位分配系统以排除异常情况，尽可能保证停车位分配系统正常使用。

通过9.2所观测的参数的可视化，可以直观地提供目标城市或地区停车场利用情况变化的信息，有助于对交通管理的进一步规划和改进。

附录 A

(资料性)

当前主要密钥系统的关键性能指标比较

目前,国内外主流的公私钥密码体系主要有:基于证书的密钥管理体系和基于标识的密钥管理体系。基于GB/T 36625.3-2021《智慧城市 数据融合 第3部分:数据采集规范》,第9.2节的技术要求和说明,此处选取了PKI作为基于证书的公私钥密码体系的代表,CCKS和CPK作为基于标识认证的公私钥密码体系的代表进行对比。

表1 当前主要密钥系统的关键性能指标比较

系统名称及类型	CCKS (公私钥矩阵密钥系统)	PKI (公钥密钥系统)	CPK (公私钥矩阵密钥系统)
用户与公私钥的关系	基于标识映射	基于 CA 证书	基于标识映射
通过第三方 (CA) 认证	不需要	需要	不需要
大规模认证能力	密钥、标识容量: 单域 10^{48} , N 个域	密钥容量: $CA+10^6$	密钥、标识容量: 10^{48} , 没有域的划分
分域精细权限管理	是	不是	不是
持续双离线认证	支持	不支持	不支持
认证速度	快	较慢	一般
建设运营成本	低	很高	较高

参考文献

- [1] ISO/IEC 30136:2018, Information technology — Performance testing of biometric template protection schemes
- [2] GB/T 36749-2018 城市可持续发展 城市服务和生活品质的指标
- [3] ISO 37122:2019, Sustainable cities and communities — Indicators for smart cities
- [4] ISO 37154:2017, Smart community infrastructures — Best practice guidelines for transportation
- [5] GB/T 43245-2023 智慧城市基础设施 数据交换与共享指南
- [6] ITU-T Y.4456:2018, Requirements and functional architecture for smart parking lots in smart cities
- [7] 彭桂林, 曹喆喆, 曹余, 无中心化离线认证技术的应用与实践[J]. 《智能建筑与智慧城市》, 2017, 250 pp. 69–72