

ICS 35.240.01

CCS A



中华人民共和国国家标准

GB/T XXXXX.1—202X/ISO 37156:2020

智慧城市基础设施：数据交换与共享指南

Smart community infrastructures —
Guidelines on data exchange and sharing for smart community infrastructures

(ISO 37156:2020, IDT)

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

目 次	II
前 言	IV
引 言	V
智慧城市基础设施：数据交换与共享指南	1
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
3.1 智慧城市基础设施	1
3.2 智慧城市基础设施数据	2
3.3 智慧城市基础设施数据交换与共享	3
4 数据交换与共享的原则	4
4.1 概述	4
4.2 原则	4
5 数据交换与共享的类型和模型	4
5.1 概述	4
5.2 数据类型	5
5.3 基础设施数据概念模型	5
5.4 数据字典和数据目录	7
5.5 数据图谱	7
6 数据交换与共享的机遇	8
6.1 概述	8
6.2 优化基础设施服务	8
6.3 促进商业发展	8
6.4 促进城市国土空间规划	8
6.5 实现主动维护	8
6.6 促进环境保护	9
6.7 提高安全和保障	9
7 数据交换与共享的安全	9
7.1 概述	9
7.2 数据安全方法	9
7.3 安全策略和原则	10
7.4 安全风险评估	11
8 数据隐私	12
8.1 概述	错误！未定义书签。
8.2 隐私指南和活动	12
8.3 隐私策略和管理	14

9 数据角色和职责	15
9.1 概述	15
9.2 数据角色	16
9.3 数据来源	16
9.4 问责制	17
9.5 新商业模式	17
9.6 合作模式的标准框架	17
附录 A 案例研究	19
A.1 基于“天地图·南京”的城市基础设施数据交换与共享	19
A.2 城市国土空间规划新模式的跨行业数据交换与共享（东京丸口地区）	20
A.3 北京万能虚拟卡应用与安全管理平台—城市基础设施数据交换与共享	20
参 考 文 献	22

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。

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。

本文件使用翻译法等同采用 ISO 37156:2020《智慧城市基础设施：数据交换与共享指南》。

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。

本部分起草单位：

本部分主要起草人：

引 言

当前，我国城市基础设施存在总量不足、标准不高、运行管理粗放等问题。加强城市基础设施建设，有利于推动经济结构调整和发展方式转变，拉动投资和消费增长，扩大就业，促进节能减排。

城市是人类技术进步、经济发展和社会文明的结晶，也是人类经济活动和区域生产的基本单位。城市基础设施可以为城市居民提供生活便利，城市功能和居民生活也依托着不同的城市基础设施。城市基础设施是城市正常运行和健康发展的物质基础，对于改善人居环境，提高居民的生活质量，增强城市综合承载能力，提高城市运行效率，提高社会效率，保障城市生态安全，稳步推进新型城镇化。科学有效的城市基础设施管理至关重要。城市基础设施管理不善则会导致环境污染、交通拥堵、城市资源不足、城市生命线系统薄弱等，对城市的可持续发展造成不利影响。

数据是有效管理的重要基础。城市基础设施数据的管理涉及多个不同的组织或部门，从而带来的信息孤岛现象对高效、便捷的管理造成了负面影响。加强数据共享对于智慧城市非常重要。标准化的数据交换与共享将有利于跨部门、跨组织和跨城市的业务协作，还将提高城市基础设施服务能力。这也将进一步夯实城市数据管理的基础，优化成果产出，使得城市更加安全、美好和宜居。

本文件主要聚焦智慧城市基础设施的数据交换与共享，可为政府、企业、组织和个人共享城市基础设施数据提供参考。本文件有助于夯实信息化基础，消除信息孤岛，推进数据利用，使城市更加智慧。例如，本文件的实施将有利于通过建立信息交换机制来促进地方政府不同部门之间的有效合作。

本文件提供了一套城市基础设施数据治理方法和遵循隐私与安全原则的城市基础设施数据交换与共享统一框架。本文件目的是：

- 为用户、消费者或受益者提供细致、高效、便捷、生态环保和安全的基础设施；
- 为城市基础设施服务的交换、监督、共享和维护提供适宜的措施。

智慧城市基础设施：数据交换与共享指南

1 范围

本文件为有权开发和运营社区基础设施的实体提供了用于数据交换与共享原则和框架的指南。

本文件适应于涉及城市基础设施数据交换与共享的所有类型的城市。每个城市依据自身特点和条件，采取合适的方法具体实施城市基础设施数据交换与共享。

注 1：根据GB/TXXXX-20XX(ISO 37100: 2016)中对城市可持续发展和韧性的定义，智慧的概念主要从数据交换与共享的角度来阐述。

注 2：附录A为城市基础设施数据交换与共享提供了应用案例。

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。

BSI PAS 183:2017 智慧城市 - 构建共享数据与信息服务决策框架的指南

3 术语和定义

下列术语和定义适用于本文件。

3.1 智慧城市基础设施

3.1.1

社区 community

城市

被授命特定责任、活动和关系的人组成的群体。

注 1：在很多场景中，但不是所有场景中，城市具有明确的地理边界。

注 2：城市是社区的一种类型。

[来源：GB/T 40758-2021, 3.2.2, 有修改]

3.1.2

城市基础设施 community infrastructure

支持城市（3.1.1）运行和活动的设施、设备和服务的系统。

注：此类城市基础设施包括但不限于能源、水、交通、废弃物和信息通信技术（ICT）。

[来源：GB/T 40758-2021, 3.6.1, 有修改]

3.1.3

组织 organization

为实现目标，在职责、权限和相互关系构成自身功能的一个人或一组人。

注 1：组织包括但不限于个体经营者、公司、集团公司、商行、企事业单位、政府机构、合股经营的公司、公益机构、社团，或上述单位中的一部分或结合体，无论其是否有法人资格，是公有企业还是私有企业。

注 2：本文件中，组织的概念指城市内负责实施管理体系的实体/机构，如：地方政府。城市确定一个组织并委托其

实施本文件。

[来源：GB/T 40758-2021，3.2.3，有修改]

3.1.4

智慧城市基础设施 smart community infrastructure

在设计、运行和维护方面具有高技术能力的城市基础设施（3.1.2），用以促进城市 and 社区的韧性和（3.1.1）可持续发展。

[来源：GB/T 40758-2021，3.6.2，有修改—删减注]

3.1.5

智慧城市基础设施数据 smart community infrastructure data

来源于各种智慧城市基础设施（3.1.4），由其产生、获取、收集或管理的数据（3.2.3）。

3.2 智慧城市基础设施数据

3.2.1

可用性 availability

根据授权实体的要求可访问和可适用的特性。

[来源：ISO/IEC 27000—2018，3.7]

3.2.2

真实性 authenticity

<实体>真实的特性。

3.2.3

数据 data

以一种适合于交流、解释或处理的形式化方式重新解释信息。

注：数据可以通过人工或自动的方式进行处理。

[来源：ISO/IEC 2382—2015，2121272，有修改]

3.2.4

完整性 integrity

准确和完备的特性。

[来源：ISO/IEC 27000—2018，3.36]

3.2.5

元数据 metadata

界定和描述其它数据的数据（3.2.3）。

[来源：ISO/IEC 27050.1—2016，3.19]

3.2.6

参考数据 reference data

领域和城市（3.1.1）标准化的数据（3.2.3）对象，用于界定一套允许值用于构成其它数据对象。

[来源：ISO 5127—2017，3.1.10.19]

3.2.7

可靠性 reliability

与预期行为和结果一致的特性。

[来源：ISO/IEC 27000—2018，3.55]

3.2.8

共享数据 shared data

可以在现有软件宜用程序以及在不同软件宜用程序之间被利用，或可被异步或同步执行的数据（3.2.3）。

[来源：ISO/IEC 2382—2015，2122341，有修改]

3.2.9

专题数据 thematic data

在数据框架内被视作对支持城市服务条款以及城市中四个级别的洞察力至关重要的数据模式。

[来源：BSI PAS 183—2017，2.10]

3.2.10

数据谱系 data spectrum

基于对数据封闭、共享或开放的考虑，对数据资产进行的利用区分。

[来源：BSI PAS 183—2017，2.4]

3.3 智慧城市基础设施数据交换与共享

3.3.1

数据获取 data access

查找、使用或检索数据（3.2.3）的权利、机会和方法。

[来源：ISO 15489.1—2016，3.1，有修改—原始词汇是“获取”]

3.3.2

数据生成者 data creator

为城市或城市服务进行数据（3.2.3）生成、获取、收集或转化的组织（3.1.3）。

[来源：BSI PAS 183—2017，7.2.2，有修改]

3.3.3

数据所有者 data owner

与城市服务相关的城市基础设施数据的指定管理者。

[来源：BSI PAS 183—2017，7.2.3，有修改]

3.3.4

数据发布者 data publisher

负责城市基础设施数据发布的组织（3.1.3）。

[来源：BSI PAS 183—2017，7.2.5，有修改]

3.3.5

数据交换 data exchange

数据（3.2.3）的获取、传输和归档。

[来源：ISO/TS 13399.5—2014，3.7，有修改]

3.3.6

数据共享 data sharing

提供可共享、可交换和可扩展数据（3.2.3）以赋能城市基础设施（3.1.2）的活动。

3.3.7

风险 risk

不确定性的影响。

注 1：影响与预期的偏离（正向的或反向的）。

注 2：不确定性是对事态及其结果或可能性的相关信息、理解或知识缺乏的状态（即使是部分的）。

注 3：风险通常被表征为事态发生的可能性（ISO Guide 73:2009, 3.5.1.3）和其后果（ISO Guide 73:2009, 3.6.1.3）或其组合。

注4：风险通常被表征为事态的后果（包括情形的变化）和相关的发生可能性（ISO Guide 73:2009, 3.6.1.1）的组合。

[来源：GB/T 40758-2021, 3.4.12, 有修改]

4 数据交换与共享的原则

4.1 概述

本文件给出在智慧城市基础设施领域应用数据交换与共享的各种可能性。城市对数据输出和使用的期望值往往非常高。然而需要注意的是，在数据交换与共享输出的范围和有效性方面存在许多不同的限制条件，例如数据的可靠性、可用性、质量、复杂关系以及对时态数据的解释。智慧城市宜根据城市基础设施数据交换与共享结果所带来的影响来设定合理的期望值。

4.2 原则

使用本文件时，宜考虑以下原则：

- a) 城市基础设施数据宜能够交换与共享。
- b) 为了确保交换与共享有效进行，宜保证数据质量以便在跨智慧城市基础设施的服务中或多个组织中使用。
- c) 数据所有者有责任和义务确保城市基础设施数据的交换与共享得以实现。
- d) 数据创建者宜维护城市基础设施交换与共享数据的完整性。
- e) 宜持续保护城市基础设施数据的安全性与隐私性。
- f) 数据宜采用空间方法来实现城市基础设施对象的定位和管控。
- g) 数据宜具备时态信息来维护城市基础设施因任何原因发生的变化，比如社会的、环境的、文化的、战略的和政策的变化。时态数据便于在需要时进行及时干预，并支持追踪城市基础设施的变化，从而实现智慧管理和效率提升。
- h) 宜采用系统的方法实现数据交换与共享，通过一套机制识别出每个数据属性，以促进城市基础设施的互操作性。
- i) 城市作为基础设施数据交换与共享的管理者，宜确保共享与交换活动是在公平公正、合乎道德的方式进行，以确保各方得到平等对待。

5 数据交换与共享的类型和模型

5.1 概述

智慧城市基础设施包括能源、水、交通、信息和通信技术（ICT）、废弃物处理服务。本文件所述是指与智慧城市基础设施和支撑基础设施的建设环境相关的数据。

智慧城市基础设施的结合发展，以及智慧城市基础设施信息服务的规划、建设、运营、管理和评估宜以数据资源的建设、开发和利用为基础。数据资源的使用宜符合ISO 37155-1规定的物理和运营条件以及相互关联。

数据交换与共享发生在智慧城市基础设施的不同应用服务和系统之间。不同类型的数据交换与共享可使用到不同的数据类型和功能。

智慧城市和社区基础设施的数据框架将数据分为元数据、参考数据或专题数据。数据框架详细描述了当前城市数据资产如何从现有的孤岛式服务过渡到数据全生命周期互通使用的形态。

数据资产集合与ISO/IEC 30182定义的数据概念有关，并运用了城市数据谱系范围内开放、共享和非开放数据的分类。

5.2 数据类型

5.2.1 元数据

元数据是定义数据属性信息，用于验证交换与共享数据的来源和有效性。例如，代表城市向市民提供城市服务的志愿服务组织有关的数据。

5.2.2 参考数据

参考数据是为要交换或共享的数据界定一套允许值的任何数据。例如，可用于多种目的的特定位置的气温读数或特定街道视频片段。

5.2.3 专题数据

以为市民提供服务为导向，城市专题数据首先宜是城市创建、处理和管理的数据集和历史数据。例如，特定街道的公交拥堵或特定地下水管道的电力频率波动和压力分布。专题数据宜考虑智慧城市基础设施的多个子系统集成特点，例如根据ISO 37155-1考虑基础设施服务之间的相互作用。

数据交换与共享主要在元数据、参考数据和专题数据之间进行。智慧城市基础设施数据交换与共享的数据类型见5.3。

5.3 基础设施数据概念模型

城市基础设施服务宜提供和收集数据，以实现交换与共享。数据的采集有望通过API支持智能电表等技术接口实现自动化。

表1至表3列出了ISO/IEC 30182中定义的与城市基础设施相关的智慧城市概念模型（SCCM）的元素。城市基础设施数据可划分为某物的特征、某物的消耗、某物的运动、某物的存在、某物的生产、某物的状态、某物的供应和某物的使用，具体见表1。这些描述包含但不限于以下情况。

表1 使用 SCCM 概念收集的城市基础设施数据示例

可收集的数据	基础设施	数据接口	数据示例	主要概念 (SCCM [®])
某物的特征	建筑 交通网络	勘测 交通网络数据 API	建筑用途 道路、桥梁或隧道的结构和设计信息	状态 基础设施
某物的消耗	街道照明	智慧电表	每小时消耗的能量（千瓦时）	实例
某物的移动	运输网络	车辆 GPS	旅程目的地	地点
某物的存在	废弃物管理	垃圾箱传感器	空/满	状态
某物的生产	可再生能源发电 厂	智慧电网	每小时能量负荷（Mwh）	实例
某物的状态	公共区域	环境传感器	室外温度	状态

可收集的数据	基础设施	数据接口	数据示例	主要概念 (SCCM ^a)
	轨道交通/地铁	地铁数据 API	地铁运行状态： 正常运行、停运或规划/在建 车辆和线轨的监测数据	状态/事件
某物的供应	水电	流量传感器	泄漏	实例
某物的使用	通信网络	系统日志	使用的数据量（兆字节）	事件
注：基础设施是服务于国家、城市或其他地区的基础性设施和系统。SCCM 未定义基础设施。然而，它是表达智慧城市基础设施数据交换与共享的基本概念。				
a：ISO/IEC 30182 中 SCCM 定义的主要概念。				

收集到的数据可转化为支撑城市洞察的信息，洞察类型在SCCM中被定义为可操作性、关键性、可分析性和战略性。这些洞察过程将有助于确定基础设施之间共享数据的时机和必要性，见表2。

表 2 基于 SCCM 收集的城市基础设施数据视角级别（可操作性，关键性，可分析性和战略性）的示例

可收集的数据	结果数据（示例）	洞察（SCCM）
某物的特征	建筑数据：尺寸、居住率、设备、室内温度、室内空气质量、供气压力、水流量、热传递温度 人口统计数据：用户注册信息和个人资料 结构或设计数据：位置、尺寸和材料；承载能力；对象中包含的功能；出口路线	可操作性 战略性
某物的消耗	能源数据：家庭用电、家庭用热（供暖）、天然气；地区消耗；关税和成本	关键性
某物的移动	运输数据：模式组合、车辆类型、车辆 ID、车载人数、旅程开始/结束时间和位置、交通速度和密度、行人活动、每公里能耗、每公里排放量/污染物	可分析性
某物的存在	图像数据：交通拥塞、道路养护等公共领域的完整性、事故、动乱和城市安全	战略性
某物的生产	能源数据：当地可再生能源生产	关键性
某物的状态	环境数据：室外空气质量、水质、洪水水位、噪音水平、温度、天气状况、碳排放量、光污染 运行状态数据：计划、建设、运行、中止、停止状态；各状态的时间段 检查数据：检查方法/负责人、检查数据、判断结果	可分析性
某物的供给	能源数据：网络功率负载	关键性
某物的使用	网络利用率：乘坐公交车的次数	战略性

观察结果与SCCM中定义的概念有关，包括行为主体或事项、度量和地点。SCCM指出，通过将时间和角色的概念添加到可收集数据中，可进一步理解数据共享的关系，见表3。

表 3 利于了解交换与共享数据关系的观察示例

可收集的数据	行为主体/事项 (SCCM)	指标 (SCCM)	地点 (SCCM)	时间	相关方角色 ^a
某物的特征 某物的消耗 某物的运动	人或家庭 建筑、基础设施或城市 政府或直辖市	成本 频率 数量	位置点 出发点 到达点	日期/时间戳	基础设施所有者、供应商和运营商 投资者

某物的存在 某物的生产 某物的状态 某物的供应 某物的使用		规模 规范 状态 速度 预期寿命	中转路线 邻里 区 市		规划师 公民
a 相关方参照 ISO 37153。					

5.4 数据字典和数据目录

数据字典和数据交换共享目录是协助不同属性(行业、结构、格式、分等)数据共享和交换的有效工具。上述工具是可选的,包括但不限于以下内容:

a) 数据字典是对某一领域内数据资源的数据项、数据结构、数据流、数据存储、处理逻辑和外部实体进行定义和描述;

b) 数据目录是数据资源组织和相关性的表述,包括目录、字典识别方案和与识别系统有关的指南的制定。数据目录形式是以开放技术字典(OTD)数据库为核心。

如果使用这些工具,基于ISO 8000和ISO 22745系列的开放式技术字典(OTD)的预期架构可用于数据的创建和维护。

5.5 数据谱系

5.5.1 概述

为了更好地实现城市数据价值最大化,宜运用数据框架对数据进行分类。数据宜根据类型和开放共享与否(非开放、可共享、开放)进行分类。数据开放共享的程度取决于安全性、访问和控制要求。谱系内数据的使用仅限于数据使用、重用和共享数据的目的。ISO 31000概述了风险管理、评估和分析方面的良好实践,可供城市实施数据框架时使用。

宜建立和实施适当的数据共享、发布和重用的风险管理制度。

5.5.2 非开放数据

非开放数据是指被限制使用的数据,且不允许被共享。在城市中,非开放数据主要是与隐私和安全有关的数据,例如:特定基础设施服务中的公民支付信息,包括市政税等。

5.5.3 可共享数据

可共享数据是指城市中存在的无法归类为开放数据或非开放数据的数据。不同城市之间共享数据有所不同,一般认为城市中大部分数据为可共享数据。

就可共享数据,本文件规定了以下内容:

----为新的目的进行数据共享的适宜性(见第8章);

----数据访问权限(见第9章)。

作为数据图谱的一部分,了解共享数据的三种顶级访问限制非常重要:

a) 特定访问是指数据所有者允许指定的个人或组织访问数据;

b) 分组访问是指根据预先确定的规则向特定人群或组织提供数据;

c) 公开访问是指可完全被公众获得的数据,仅在特定条款或条件下被视为不公开。

受限数据共享发布前,城市数据发布者有责任考虑到该类数据共享对个人或资产造成的潜在危害,此类可共享数据的例子如控制重大事故和危害(COMAH)数据。

5.5.4 开放数据

本文件使用开放项目提供的“开放”定义。

开放数据是指任何人均可以任何目的自由访问、使用、修改与共享的数据，最多遵守保护来源和开放性的准则。该定义也被用来确定数据是否可以被归类为开放数据。

6 数据交换与共享的机遇

6.1 概述

开放数据的可用性使得智慧城市能够探索数据的价值以改善城市服务。然而，出于隐私和安全的考虑，智慧城市中的大多数数据不适合开放。通过适当的访问限制，可以解锁三种类型的共享数据，以造福城市及其市民。共享数据的价值包括但不限于优化基础设施服务、促进商业发展、促进城市国土空间规划、实现主动维护、促进环境保护和提高安全保障。当城市基础设施数据实现共享时，可以为所有智慧城市提供多种选择。

6.2 优化基础设施服务

数据交换与共享可以为市民提供更好的服务，包括水、气、电、住房、交通、垃圾处理和信息服务。例如，通过政府部门之间的数据交换与共享，市民可以获得一站式、全面和高效的政府信息服务。

通过数据交换与共享，城市管理者及相关的公共服务提供者不仅可以优化城市基础设施建设，而且可以提高城市基础设施日常管理以及运营监控的效率。例如，路灯柱作为共享基础设施，既可以作为充电点为电动汽车提供能源，也可以配备广告牌。通过在路灯柱上安装各种传感器或摄像头，可以监测交通、噪音水平和天气状况。确保此类信息可共享具有重要意义。

6.3 促进商业发展

数据交换与共享能够提高资源配置效率，促进商业发展。例如，开发商可以利用来自城市基础设施的共享数据，获取其通信能力、供水能力以及车站之间的乘客数量，来探索建造新酒店的最佳位置，以最大限度降低开发成本。

数据交换与共享为城市商业模式的创新提供了机遇。例如，将交通数据和市民的一般出行情况结合起来，可以用于打造无人驾驶出租车业务。

6.4 促进城市国土空间规划

数据交换与共享可以帮助城市国土空间规划者制定全面的基础设施规划，提高城市空间的开发利用水平，实现城乡基础设施的平衡，使城市更加和谐宜居。

通过数据交换与共享，可以实现相邻基础设施之间的控制和避让要求，有效避免规划失误，减少基础设施容量不足引起的问题，提升政府行政审批效能。例如：通过数据共享，可以在供电管道与输气管道之间保持一定的垂直和水平距离，以确保安全。

数据交换与共享可以帮助城市管理者制定基础设施协同实施计划。通过各种基础设施的协同建设，促进城市国土空间规划和管理精细化，避免盲目开挖、重复建设和资源浪费。

6.5 实现主动维护

数据交换与共享可以用于更高效和更有预防性的智慧城市基础设施维护，可以及时向基础设施所有

者、决策者、运营商或其他相关方提供基础设施运行状况的相关信息，并发现缺陷或故障的最初征兆，从而实现高效、低成本的操作和维护活动。

对收集到的数据进行额外分析可以进行预测性维护，旨在为维护活动节省有效的预算、规划和成本。通过收集的数据可实现主动维护。共享数据还宜提高基础设施运行的安全性，实现智慧城市基础设施的有效运行。例如，结合道路交通数据和人流量，可以通过调节路灯开关时间，以节省能源并提高运营和维护计划的效率。

6.6 促进环境保护

智慧城市基础设施数据的交换与共享可以促进环境保护。通过数据交换与共享，在城市基础设施服务的设计中可以限制污染程度、更高效地利用材料和能源等资源、减少废弃物，还有利于减少基础设施对现有绿地（如公园、湿地、河道缓冲区、步行道等）及地表径流和排水的影响。

数据交换与共享也有助于改善公共健康。例如，通过共享空气质量数据、供暖数据以及交通数据，可以帮助城市管理者采取适当的采暖和交通管控措施，以避免空气质量恶化。

6.7 提高安全和保障

城市基础设施数据可用于提高城市服务的安全性。例如，利用天然气管道、通信线路和电力线路的地理位置相关数据，能够帮助城市管理者进行灾害管理。这可用于地震、火灾、洪水和其他自然灾害。数据共享可以帮助政府更加有效地处理紧急情况。

7 数据交换与共享的安全

7.1 概述

智慧城市的基本前提是宜更多地利用来自城市基础设施的可用数据进行交换与共享，以最大限度地提高城市服务提供的可用性、可靠性和韧性，造福于市民。

技术的使用推动了基于数据交换与共享服务的改进。然而这增加了对此类技术的依赖，特别是当该技术用于新服务交付模式时。这还会造成严重的漏洞和相关安全问题。

接口是数据交换与共享中特别敏感的部分。对接口加以特殊考虑并用必要的安全技术保护数据和设置访问权限很重要。数据访问权限宜仅限于经过授权和审查的一小群人。

智慧城市的多机构和组织参与模型是由数家能提供不同城市基础设施的机构和组织组成。在此模型中，所有参与提供基础设施的机构和组织均有责任维护数据交换与共享安全。

确保智慧城市数据安全所需的方法与已存在的城市基础设施内单个服务级别的安全政策和流程不同。智慧城市基础设施的数据安全需要应对由可用数据的共享和交换而导致的新的或增长的威胁。

7.2 数据安全策略

交换与共享的城市基础设施数据的安全，需要采取整体的适应整个城市范围的策略，此策略宜适当且符合实际应用，并有助于实现城市愿景和目标。为了确保整体数据安全，所用安全措施需要考虑到城市基础设施服务的物理、网络、人员和信息物理方面的安全。这意味需要将数据交换与共享安全作为一个整体来对待且避免单独制定安全计划。

实现城市基础设施数据安全的一个关键方面是，需要考虑来自跨越单个服务供应方边界（例如交通、水或废物）城市服务的数据安全，并为整个城市服务提供有效和安全的数据使用。

宜采用全面而适当的数据安全措施，以阻止和消除威胁城市基础设施的敌对、恶意、欺诈和犯罪行为

为或活动。安全方法宜设法保持数据的机密性、完整性和可用性，尽可能确保数据避免非计划内的访问与使用的危险或威胁。

城市基础设施数据交换与共享的漏洞来自于：

- 各基础设施服务供应方的组织优先次序不同；
- 管理方式、政策和过程与基础设施供应方不兼容；
- 城市基础设施数据与来自城市内外更广泛数据聚合；
- 城市基础设施供应方之间对安全的理解和关注程度不同；
- 城市和社区基础设施供应方管理数据安全风险偏好范围不同。

生成、收集、利用和存储数据的数量和速度的加快，增加了城市基础设施数据的安全漏洞。安全措施需要考虑个人资料、知识产权及商业敏感资料的交换及共享要求（例如使用者取得交换与共享资料后的目的及后续用途），为全市服务提供便利。

数据存储需要特殊考虑，例如数据分散存储可能比集中存储更安全。宜避免数据重复存储。

考虑来自试图突破城市基础设施数据安全措施漏洞行为者的威胁是很重要的。这些行为者可能与有组织犯罪有关并试图获取未经授权的个人或敏感数据、知识产权或商业敏感数据。必需考虑潜在的恐怖主义行为，因这些犯罪者试图通过破坏城市数据的交换和/或共享而破坏城市服务或危及城市基础设施或市民的安全。

7.3 安全策略和原则

7.3.1 概述

一个智慧城市要获得并保持公众信任，需要能够回应公众对城市基础设施数据交换与共享日益提高的意识和任何潜在的担忧。城市宜准备好建立适当机制以维持市民信任。关于城市数据如何被使用，城市需要有能力和应对日益增长的公众意识和潜在担忧，并建立机制来防止公众信任受损。

在确定适当的城市基础设施数据安全治理时，安全措施需要考虑居民、游客和那些能够提供有效城市服务的市民。

7.3.2 安全策略

城市宜提供不同的服务选择。城市基础设施供应方的所有权可能很复杂并将影响所采用的数据安全措施。城市在设计实施恰当的数据安全措施时，需要考虑服务供应方的自主权。

城市制定数据安全策略需要考虑城市基础设施的安全实施和所用服务的所有方面，特别是：

- 数据交换与共享的安全；
- 交换与共享数据的真实性；
- 城市基础设施数据的可用性、来源和可靠性；
- 服务数据的机密性和商业敏感性；
- 确保交换与共享数据完整性的恰当措施；
- 交换与共享数据的弹性要求；
- 接口是数据交换与共享的敏感部位和需要设置数据访问权限的事实。

城市需要制定阐明城市基础设施总体安全政策的安全策略，详细说明被共享和交换的数据是哪些，以及如何收集、管理和处理这些数据。该安全策略还宜考虑适用于城市管辖的法规和条例。还可考虑以安全策略为基础，制定和实施其他城市基础设施服务，以有益于公民。

7.3.3 安全原则

城市基础设施数据交换与共享需要考虑的数据安全措施宜包括下列主要领域：

- 治理；
- 服务人员；
- 市民；
- 提供服务的组织；
- 恰当和相称的全市安全流程；
- 城市服务所需要的物理安全。

重要的是要确保数据安全措施是在城市基础设施的复杂性和基础设施运行的城市规模背景下设置的。数据访问权限宜限制在小而可靠的群体中。

7.3.4 义务与责任

一个城市采用的数据安全方式，宜能为城市基础设施供应者提供一个适当、可用于多机构的模式，而且这种安全方式还可以支持数据框架的开发，使该城市能确定每家城市基础设施服务供应方的义务和责任。

随着安全的数据交换共享的数据框架逐步成熟，城市决策者宜认真思考应对这些不断变化的数据格局。数据框架的改变可由许多原因所致，包括：

- 引入新的城市基础设施；
- 现有服务合同变更。

这种数据安全方式的好处是城市将管理日常共享和交换的数据，因而能理解正常的操作程序。这能帮助城市管理层确保城市服务供应方对城市基础设施数据的安全共享、处理和交换负起责任。

7.4 安全风险评估

7.4.1 威胁

智慧城市管理层需要了解他们所在城市有哪些威胁需要缓解。需要了解城市面临的威胁范围和潜在漏洞，其中可能包括：

- 破坏或贪污城市基础设施服务数据；
- 丢失与城市基建服务有关的个人数据、知识产权或商业敏感数据；
- 泄露城市基础设施服务的使用、运作或价值的的数据；
- 来自于一个或多个组织针对全市范围内与城市基础设施数据交换和/或共享的相关漏洞；例如，针对整体运输和交通管理服务数据的漏洞；
- 通过内部或外部攻击产生的蓄意破坏；例如，来自恶意软件、黑客或心怀不满的人员的破坏；
- 因网络物理系统导致城市物理基础设施物理性损坏；
- 盗窃、勒索、未经授权使用城市基础设施服务所致城市基础设施服务损坏或中断；
- 操作风险，如对电动无人驾驶车辆(EDV)的攻击，影响EDV程序的未知漏洞、因支持EDV运行设施复杂性的威胁、或其他因EDV或相关车辆基础设施所导致的意外障碍的威胁；
- 金融风险。

对威胁模式的评估，宜考虑攻击可能导致城市基础设施服务供应方交换与共享的数据，丧失机密性、可用性、安全性、韧性、所有权、真实性、实用性和/或完整性。

城市管理层宜考虑任何潜在的不安全或因维护服务不善，导致被交换与共享的数据泄漏、暴露或未经授权的访问。对这些基础设施服务的攻击可能导致整个城市脆弱性增加。

宜与城市基础设施服务供应方鉴定合同，以实现数据交换与共享的互操作。重要的是要考虑这些合

同是否给予了对其他组织的知识产权和/或商业敏感数据的额外访问权限，或将访问基础设施数据的权限扩展至那些尚未列入现行合同的服务供应方。

7.4.2 安全风险

7.4.2.1 概述

需要对所有城市基础设施服务的安全风险进行有效管理。城市管理宜确保对与城市基础设施服务提供的数据访问相关的所有关系进行专门管理，以减轻已确定的安全风险。

7.4.2.2 个人数据

为了提供可互操作的城市基础设施服务，城市可能会在比目前更多的组织之间交换与共享个人数据。个人数据安全事件可能危及市民、基础设施机构和组织，并可能损害市民对机构和组织的信任，对整个城市造成负面影响。

7.4.2.3 元数据

元数据提供有关城市交换与共享数据的信息，例如用于数据框架中的数据使用和访问规则。该城市基础设施元数据成为一种额外的安全风险。涉及元数据的安全漏洞将暴露城市基础设施数据如何被管理的关键细节。宜引入特殊的安全措施以确保元数据的有效管理。

7.4.2.4 参考数据

参考数据不需要定期更新，其内容也不用定期更新。例如，传感器的允许差或关键建筑物的位置。然而，攻击这些数据的潜在影响将波及整个城市，并可能对城市基础设施服务产生重大影响。宜采取特殊的安全措施以确保参考数据的有效管理。

7.4.2.5 聚合数据

为了提供、监控和维护城市基础设施服务，宜对交换与共享数据进行聚合。这种聚合可能导致个人、个人团体和组织面临增加的风险和敏感性。数据的特定组合或缺失可能会允许直接或通过推理而识别出公民身份，从而将这些公民置于危险之中。宜引入特殊安全措施，以确保对聚合数据的有效管理。

重要的是，任何对聚合交换与共享数据的风险研究，都要考虑所需的安全措施，以减轻聚合数据被用于生活模式恶意分析的威胁。

8 数据隐私

8.1 概述

数据隐私与所有智慧城市基础设施相关的数据安全的准则同等重要。数据隐私适用于所有个人数据或能用于构建公民个人数据的数据。

智慧城市的多机构模式由许多不同的机构组成，每个机构都有责任提供城市服务，并分担保护公民数据隐私的责任。

本文件规定的隐私指南仅限于智慧城市基础设施使用的数据的交换与共享。

8.2 隐私指南和活动

8.2.1 概述

本文件中详述的数据隐私保护内容，供智慧城市使用，确保与提供城市基础设施服务的个人和组织相关的数​​据，得到隐私保护和保密。具体而言，这些隐私保护指南涉及那些参与智慧城市中智慧城市基础设施数据交换与共享的组织。

8.2.2 隐私原则

下列八项数据保护原则，宜用于交换与共享涉及个人数据或能被推断出个人数据的智慧城市基础设施数据：

- 在其所申请应用的司法管辖区内公平地处理；
- 仅为特定目的而获取并不进行与此特定目标不符的进一步处理；
- 充分性、相关性和适度性；
- 准确的和最新的；
- 保存时间不超过必要时间；
- 依据所赋的个人权利处理，包括数据访问权；
- 保持安全性；
- 不转交给所申请应用的司法管辖区之外那些未经充分保护的国家或地区。

如果智慧城市已经确定除上述八项隐私原则之外的任何豁免条款，这些豁免条款宜被记录在案并告知其所采用的每个智慧城市基础设施服务予以确认。

参与智慧城市基础设施数据交换与共享的每个组织，宜确保在其采用的智慧城市基础设施服务的要求和指南内执行这些隐私原则。

8.2.3 城市相关方的考虑

在每个城市的基础设施服务的设计、建设和实施过程中，八项隐私原则宜用于所有智慧城市和社区基础设施服务的数据交换与共享。宜考虑所有相关方，例如公众、病人、学生、客户、供应商、商业伙伴和城市服务组织。

在城市和社区基础设施服务实施的所有阶段，宜确定数据所有者、数据发布者和服务使用者角色，并与隐私保护原则一起考虑。宜确定组织并明确其所负有的数据责任。此外，宜设置适当机制以促进智慧城市基础设施数据交换与共享的保密性。

智慧城市宜确保清楚识别和记录，因智慧城市基础设施服务运行而由城市服务机构处理的高风险类别的个人信息。

高风险类别的个人数据可包括：

- 由立法或监管机构确定的敏感的个人​​信息；
- 个人银行账户和其他财务信息；
- 身份证号，如国民保险号码；
- 与弱势成人和儿童有关的个人信息；
- 个人的详细资料；
- 可能会对个人产生不利影响的敏感商谈。

智慧城市宜考虑到处理大量个人数据的智慧城市基础设施服务，并恰当管理这些情况下增强的风险。

8.2.4 特殊的专题数据

参与数据交换与共享的每个智慧城市基础设施组织，宜有其自己的指导原则以保护与服务相关的数据，如知识产权或商业敏感数据。当为每一项智慧城市基础设施服务开发适当的数据交换与共享机制时，宜考虑这些组织。为了维护隐私和安全，何时宜考虑特定的数据指南是重要的。如果这些数据被无意或故意地公开，那可能不仅对个人或城市服务产生影响，而且会对整个城市产生影响。

8.2.5 操作指南

智慧城市基础设施系统一旦实施，就形成了关键的城市服务。智慧城市期望应用城市管理、部分或所有这些服务的个性化和定制化。在这些服务的运行中，可能会改变管理数据交换与共享的隐私机制、规则和政策。宜对明确的角色和责任进行管理，以便能恰当反映所必需的任何改变。这些改变宜支持各方面管理策略的更新，如：

- 内部服务规则的更新；
- 组织间的交互规则；
- 操作过程的更改；
- 保护措施，如定义新角色；
- 改变数据访问管理规则；
- 维护责任。

在上述每种需要改变操作的情况下，城市宜确保这些更改也包括了认证、授权、访问和审计规则的检查。

8.3 隐私策略和管理

8.3.1 高层管理小组

智慧城市宜确保由高层管理小组负责发布和维护隐私政策，该项政策具有明确的框架和示范支持并执行智慧城市基础设施数据的交换与共享。其中宜包括，管理数据保护立法和规章制度的合规性及良好的实践应用性。

8.3.2 隐私政策

隐私政策宜说明其涵盖以下任一方面：

- 整个城市和履行服务的组织；
- 或被认证的参与智慧城市基础设施服务设计、建设、实施或交付的组织。

宜将隐私政策传达到所有交付该城市智慧城市基础设施服务的负责人。

8.3.3 义务和责任

城市宜指定一名高级管理团队的成员对城市服务的隐私指南负责。指定的团队成员宜负责管理城市隐私数据的交换与共享。该团队成员还宜遵守数据保护立法和法规，并努力展示和推广良好的隐私行为制度。

智慧城市及其服务的复杂性，可能需要许多工作人员专门负责，建立恰当的数据交换与共享政策以及合规活动。隐私程序宜确保城市服务组织如下处理个人数据：

- 公平的情况下；
- 仅在合理的情况下；
- 仅在为城市服务组织的目的并考虑到适用于恰当管辖范围内的任何立法或条例的必要情况下。

宜向对城市提供个人信息的任何个人或组织提供交换和数据共享规则访问权限。该城市宜出具一份

隐私通知，明确传达以下信息：

- 城市服务组织的身份；
- 数据被交换、共享或处理的目的；
- 交换与共享数据披露给第三方的相关信息；
- 交换、共享和处理数据时，个人访问个人数据权限的有关信息；
- 个人数据是否在没有充分保护的情况下转移到立法或监管辖区之外；
- 如何联系城市查询有关交换或共享数据处理的详细信息；
- 用于网站上收集个人数据的任何技术的详细信息，例如cookies；
- 可使处理公平的任何其他的信息。

8.3.4 隐私处理流程

智慧城市宜纳入隐私流程，确保任何城市组织与其他城市组织共享个人数据，以提供城市服务。双方在交换或共享数据方面的责任符合智慧城市隐私政策。这些隐私处理流程宜在书面数据协议或酌情签订的合同中正式记录。

隐私处理过程宜包含确保每个组织正在使用数据提供城市基础设施服务的程序，

- 书面协议或合同描述可能被使用数据的目的以及对数据使用的任何限制或制约；
- 每个组织提供一份承诺书或证据，证明其承诺以不违反智慧城市隐私政策的方式处理数据。

隐私政策宜纳入程序，以确保在可能的情况下，任何涉及与第三方交换或共享数据的新处理，都符合本市隐私通知政策及提供给个人的隐私通知条款。

如果无法做到这一点，城市基础设施组织宜确保在必要时获得个人对数据交换与共享的同意。

如果允许在未经个人同意的情况下与第三方进行数据交换与共享，则隐私过程宜包含一些程序，确保该数据交换与共享的协议和限制条件具有可审计记录。

在需要与第三方交换与共享数据的情况下，如立法要求，隐私过程宜纳入确保数据协议和控制的程序。

8.3.5 个人的隐私权

无论谁个人数据的创建者，认识到个人对自己的数据拥有权利是很重要的。隐私保护程序应包括确保尊重个人及其数据权利的程序，以及确保在任何法定时限内处理其行使这些权利的要求。隐私权包括访问信息、反对处理和审查自动化处理。

8.3.6 投诉和申诉

隐私程序宜包含一个投诉程序，以确保有关个人数据交换、共享或处理的投诉得到正确处理。这宜包括考虑到个人就其投诉处理方式提出的申诉程序。

9 数据角色和职责

9.1 概述

智慧城市相关的数据可包含由各种固定和移动终端、传感器、摄像机和应用程序定期自动收集的市民行为、位置、轨迹和通信记录。

随着持续收集，数据的价值不断增加，数据的安全威胁也在增加。数据角色和职责宜清晰，包括促进隐私和安全措施的相关责任。

9.2 数据角色

尽管各个城市都有自己的数据价值链，但为了最大程度地发挥数据框架在城市中的影响力，需履行五个关键角色的职责。跨数据价值链中存在的角色包括。

a) 数据生成者

数据生成者角色定义了那些为城市或其自身服务收集和/或转换数据的组织。此角色可以是一个被动的角色，即作为为城市提供服务的一部分，负责为城市创建数据，如创建与城市路灯灯柱位置有关的城市数据。此外，此角色可以是一个反应式的角色，即收集和转换城市运营数据并提供关键洞察，如城市中的交通运营商在发生严重事故时提供摄像机收集的数据。对于将其他人创建的数据转换为衍生或聚合数据，数据创建者是这一转换过程的提供者。

b) 数据所有者

数据所有者代表城市对城市服务相关数据进行管理。此角色的职责包括在适当情况下更改数据的权限，并代表城市在数据框架内保持数据来源的透明度。

c) 数据保管者

与数据所有者不同，数据保管者不拥有数据，而仅是在城市内为特定目的或任务提供相关服务的数据保管人。

d) 一级发布者

此角色一般指对跨数据图谱的所有数据进行发布的组织。承担一级发布者角色的组织可以查看所有数据源，但是可能不会发布所有数据。数据的发布取决于数据所属的数据图谱以及相应的访问限制。

e) 二级发布者

在智慧城市中，还存在次一级的发布角色。一级发布者推进了数据领域中的部分数据的发布，而在此基础上，对于某些已发布的数据，某些组织可以从已发布的城市数据中创建附加的价值。宜鼓励这些二级发布者发布经其创建的具有新价值的数据。作为数据发布过程的一部分，二级发布者宜监测数据框架中的数据质量，并将数据发布过程中检测到的任何差异反馈给城市。二级发布者对数据的访问权限宜由一级发布者确定。宜建立一个反馈闭环，来支持一级发布者将权限授权给二级发布者，以监督数据本身的发布。

f) 使用者

许多在数据价值链中扮演不同角色的组织，可同时被认定为城市数据的使用者。尽管这在不同城市之间有所不同，但是所有城市都有共同的关键使用者群体。他们是：

- 支持城市服务运营的城市组织，例如应急服务、城市医疗卫生服务及承包商；
- 提供或支持城市服务的第三方组织；
- 商业使用者，例如企业和中小企业；
- 市民；
- 学术组织；
- 其他城市。

9.3 数据来源

数据框架中的元数据和参考数据宜具备城市专有属性，理解数据的来源对于有效交换与共享城市基础设施数据至关重要。通过确保智慧城市基础设施数据的可查找性、可访问性和互操作性，可以释放城市数据的价值，具体如下：

- 可查找性：确保数据可被发现和识别的机制。
- 可访问性：适用于数据使用的许可和/或许可限制，以及如何使数据可供第三方使用。

- 可互操作性：数据可供所有组织使用或重复使用的程度。

数据框架提供了一个实用的工具，作为智慧城市基础设施数据的清单，协助城市管理者识别共享和交换智慧城市基础设施数据的潜在影响和收益。

- 数据质量：数据的一组固有特性满足要求的程度。

注：要求是指规定的需求或期望，通常是隐含的或强制性的。

9.4 问责制

数据所有者负责确保数据收集、交换与共享过程在所有城市基础设施中以一致的方式实施，特别是在元数据和参考数据的底层定义、数据质量、协议和格式方面。

城市相关方会遇到一些普遍问题，这些问题是由长期存在的数据孤岛所造成，例如：

- 碎片化的数据集；
- 不同的时间框架；
- 不同的空间足迹；
- 不同的颗粒度；
- 不同的格式及专有格式；
- 相同数据集的不同定义；
- 共享的积极性较低。

因此，所有权和相关知识产权的问题可能成为城市基础设施数据交换与共享的障碍，并成为数据框架中价值实现的障碍。

尽管如此，提供城市基础设施服务之间的数据交换与共享符合城市数据所有者的更广泛利益，其可促进对城市基础设施的投资，从而最大化城市绩效，降低成本，调和市民需求，支持城市管理，保护环境以及促进可持续发展和城市韧性。

9.5 新商业模式

有许多新的商业和商业模式可以支持创建数据框架，并克服遗留的数据孤岛问题。

其中一个例子就是城市数据合作社，它指的是一个负责任的可信赖的合作伙伴。这种商业模式将成为提供合作框架的机制，以开发和支持智慧城市基础设施数据的一系列质量和责任协议。构建城市数据合作社，可以减轻基础设施之间数据交换与共享的负担。这些组织将创建质量协议，提供可用的数据格式，以最大化交换与共享智慧城市基础设施数据的好处。

鉴于基础设施所有者、供应商和运营商使用由城市活动和互动产生的数据，城市宜继续围绕达成一致的标准开发用例，从而为支持良好数据治理搭建实用模板和流程。

9.6 合作模式的标准框架

合作数据交换与共享的标准框架宜包括接口、过程处理、整合、度量以及城市各领域和组织的规模影响评估。可通过对组织的剖析和利用SCCM在ISO/IEC 30182中定义的概念来实现。其他接口（如设备和仪表）的技术标准已经完备。

整合标准包括数据的技术整合和管理，以及在数据控制者、处理者、集成商和供应商之间进行相互依存的角色分配，从而支持城市的立法和监管管辖权。

关于影响的度量，相关智慧城市指标（例如，ISO 37120中建议的智慧城市指标）有助于解释SCCM在ISO/IEC 30182中定义的运营、分析、战略、关键等四个层次的影响洞察。

为对影响进行更好把握，对影响程度进行评估的标准宜与ISO 37153保持一致。

这是一个复杂而服务完备的标准领域。BSI PAS 183: 2017 应该用于指导智慧城市基础设施数据的交换与共享。

附录 A
(资料性)
案例研究

A.1 基于“天地图·南京”的城市基础设施数据交换与共享

项目名称	基于“天地图·南京”的城市基础设施数据交换与共享	
项目概况	<p>随着信息化建设和智慧城市的不断发展，政府部门对空间信息的应用需求也在不断提升，对于数据共享的需求非常强烈。基于“天地图·南京”，南京市政府搭建了城市基础设施公共服务平台，构建了各类城市基础设施数据一张图。平台提供了门户网站、标准服务、API开发、前置服务器、移动APP等多种共享模式，实现了城市基础设施数据的交换与共享。平台在智慧城市中也发挥着重要作用，主要包括门户网站、数据管理系统、服务发布系统、目录与数据交换系统、运行管理系统和协同管理系统。</p> <p>本案例构建了智慧城市基础设施数据体系，可以为数据集成、综合和管理提供服务，形成了数据交换与共享框架。在保障全生命周期数据安全的基础上，完成智慧城市基础设施数据的交换与共享。</p> <p>在数据类型方面，平台构建了涵盖“能源、水、交通、废弃物、ICT”的城市基础设施数据体系，并且进行了要素细化。除了地理信息属性，城市基础设施还包含丰富的专题信息和参考信息。数据管理系统可以实现多种类型、多种格式的数据有效组织与管理。</p> <p>在数据融合方面，目录与数据交换系统基于网络目录服务规范，提供服务注册、发现和绑定，实现国家、省、市级城市基础设施服务的互通。基于“天地图·南京”，平台能实现轨道交通、污水雨水等领域的数据集成、综合和管理，并形成城市基础设施数据一张图。</p> <p>在数据交换与共享框架方面，服务发布系统提供在线信息服务，支持使用常规开发语言构建基于服务的应用系统。平台提供了门户网站、标准服务、API开发、前置服务器、移动APP等多种共享模式。</p> <p>在数据安全方面，运行管理系统实现了平台用户和权限管理、服务管理以及服务应用的运行状态监控。</p>	
地点	中国南京	
时间	2016年至2017年	
参考文件	无	
与本文件的相关性	6.4	促进城市国土空间规划
	6.5	实现主动维护
	9	数据角色和职责

A.2 城市国土空间规划新模式的跨行业数据交换与共享（东京丸口地区）

项目名称	城市国土空间规划新模式的跨行业数据交换与共享（东京丸口地区）	
项目概况	<p>本项目是一个试点项目，利用东京丸口地区跨行业数据资源来创建城市国土空间规划新模式。参与者包括城市开发商、ICT服务供应商、通信服务供应商和学术界。</p> <p>要共享的数据：</p> <p>在本项目中，各公司的行业数据都与其他参与组织共享。例如，城市开发商提供其建筑能耗数据、租户店铺的销售额和客户属性数据；通信服务供应商提供该区域人员流动数据；其他许多与该区域相关的开放数据也被共享。</p> <p>如何交换与共享数据：</p> <p>共享是在数据交换和利用平台上进行的，使用的是ICT服务供应商提供的区块链技术。数据提供者在平台上注册数据的属性信息，以通知其他人他们拥有什么样的数据。参与者就能结合这些数据创造新的业务或服务想法，然后通过深入分析数据，得到这些数据的相关性。</p> <p>数据利用的预期效果：</p> <p>该项目旨在验证来自不同行业的数据的组合能为企业和服务创造新的价值。例如，可以将办公楼的能耗数据与人流数据相结合，为商店策划有效的推广活动。</p> <p>未来的前景：</p> <p>该项目向提供数据或分析技能的新公司开放，以便多种数据的共享和利用，不仅能用于提供新的服务，还能用于研究城市国土空间规划的新模式。</p>	
地点	日本 东京丸口地区	
时间	2018年5月至2018年12月	
参考文件	https://www.fujitsu.com/global/about/resources/news/press-releases/2017/0605-01.html https://www.fujitsu.com/global/about/resources/news/press-releases/2018/0514-02.html	
与本文件的相关性	4	数据交换与共享的原则
	5.1	概述
	5.4	数据字典和数据目录
	5.5	数据图谱

A.3 北京万能虚拟卡应用与安全管理平台——城市基础设施数据交换与共享

项目名称	北京万能虚拟卡应用与安全管理平台——城市基础设施数据交换与共享安全案例	
项目概况	<p>在北京，需要使用移动虚拟卡来执行不同政府部门的发布和管理，以及公民日常的衣食住行、娱乐、教育、医疗以及支付水、电和燃气费用。在提供方便、低成本访问这些活动的过程中，需要保证公民身份信息的安全。</p> <p>北京虚拟卡安全管理平台是基于虚拟卡持卡人，在交易安全屏障保护过程中应用终端，进行唯一身份认证、加密和虚拟卡在交易过程中的安全容垒保护；利用去中心化的离线认证模式、在线维护、虚拟卡和虚拟POS的安全管理，降低整体运营成本及社会成本和现有信息与数据安全威胁的风险。通过这些方式，北京通虚拟卡应用和安全管理平台为城市分析和决策提供了大数据来源，形成了城市基础设施数据交换共享的互信和安全保障机制。</p> <p>北京通虚拟卡安全管理平台主要包括三部分：1)基本保障系统；2)虚拟卡系统；3)数据运营平台。</p> <p>在安全设计方面，该项目遵循保护最薄弱环节、完整性、一致性、最低权限、可操作性、技术与管理相结合等相关安全设计原则。</p> <p>在交易安全保护上，采取了匿名技术、身份标识认证技术、防复制和防伪等技术。</p> <p>在网络系统安全方面，该项目将网络域划分为不同的安全级别的部分，其中防火墙和访问控制策略限制了非法访问。利用网络评估系统和入侵检测系统对网络安全事件进行检测和评估。</p> <p>通过提供ECC芯片、安全容垒和生命周期管理的可靠保证技术，为虚拟卡的发行、流通和交易提供了安全可靠的应用环境。</p> <p>为了确保应用系统的数据库系统安全，如交易和通信安全、用户访问控制和数据安全，本项目使用了强大的加密技术——非对称密钥系统、组合信用密钥系统(CCKS)，无需第三方认证中心(CA)的支持即可实现身份识别，可支持物联网离线认证和实时防伪，部署迅速且成本较低。</p> <p>此外，预访问服务系统用于访问虚拟卡SDK，该SDK提供对虚拟卡的帐户管理和交易服务的访问。交换系统可以采用多节点、多处理的方式进行部署，如请求路由处理、交易处理、交易过程管理等。</p>	
地点	北京	
时间	2016年至2017年	
参考文件	无	
与本文件的相关性	7.2	数据安全方法
	8.2	隐私指南和活动
	9	数据角色和职责

参 考 文 献

- [1] GB/T 40758-2021 城市和社区可持续发展 术语
- [2] GB/T 40759-2021 城市和社区可持续发展 可持续发展管理体系 要求及使用指南
- [3] GB/T 36749-2018 城市可持续发展 城市服务和生活品质的指标
- [4] GB/T 20988-2007 信息安全技术 信息系统灾难恢复规范
- [5] GB/T 25056-2018 信息安全技术 证书认证系统密码及其相关安全技术规范
- [6] GB/T 33132-2016 信息安全技术 信息安全风险处理实施指南
- [7] GB/Z 42192-2022 智慧城市基础设施 绩效评价的原则和要求
- [8] ISO 37122, *Sustainable cities and communities — Indicators for smart cities*
- [9] ISO 37123, *Sustainable cities and communities — Indicators for resilient cities*
- [10] ISO/TR 37150, *Smart community infrastructures — Review of existing activities relevant to metrics*
- [11] ISO 37153, *Smart community infrastructures — Maturity model for assessment and improvement*
- [12] ISO 37155-1, *Framework for integration and operation of smart community infrastructures — Part 1: Recommendations for considering opportunities and challenges from interactions in smart community infrastructures from relevant aspects through the life cycle*
- [13] ISO Guide 73:2009, *Risk management — Vocabulary*
- [14] ISO 5127:2017, *Information and documentation — Foundation and vocabulary*
- [15] ISO 8000-2, *Data quality — Part 2: Vocabulary*
- [16] ISO 8000-110, *Data quality — Part 110: Master data: Exchange of characteristic data: Syntax, semantic encoding, and conformance to data specification*
- [17] ISO 9000, *Quality management systems — Fundamentals and vocabulary*
- [18] ISO 10845-5, *Construction procurement — Part 5: Participation of targeted enterprises in contracts*
- [19] ISO/TS 13399-5:2014, *Cutting tool data representation and exchange — Part 5: Reference dictionary for assembly items*
- [20] ISO 15489-1:2016, *Information and documentation — Records management — Part 1: Concepts and principles*
- [21] ISO/TS 19163-1, *Geographic information — Content components and encoding rules for imagery and gridded data — Part 1: Content model*
- [22] ISO 22745-1, *Industrial automation systems and integration — Open technical dictionaries and their application to master data — Part 1: Overview and fundamental principles*
- [23] ISO 31000, *Risk management — Guidelines*
- [24] ISO/IEC 2382:2015, *Information technology — Vocabulary*
- [25] ISO/IEC 11770-1, *Information technology — Security techniques — Key management — Part 1: Framework*
- [26] ISO/IEC 11770-3, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*
- [27] ISO/IEC 15946-1, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 1: General*
- [28] ISO/IEC/IEEE 24765, *Systems and software engineering — Vocabulary*

- [29] ISO/IEC 25066, *Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — Common Industry Format (CIF) for Usability — Evaluation Report*
- [30] ISO/IEC 27000:2018, *Information technology — Security techniques — Information security management systems — Overview and vocabulary*
- [31] ISO/IEC 27001, *Information technology — Security techniques — Information security management systems — Requirements*
- [32] ISO/IEC 27002, *Information technology — Security techniques — Code of practice for information security controls*
- [33] ISO/IEC 27003, *Information technology — Security techniques — Information security management systems — Guidance*
- [34] ISO/IEC 27004, *Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation*
- [35] ISO/IEC 27005, *Information technology — Security techniques — Information security risk management*
- [36] ISO/IEC 27033-1, *Information technology — Security techniques — Network security — Part 1: Overview and concepts*
- [37] ISO/IEC 27050-1:2016, *Information technology — Security techniques — Electronic discovery — Part 1: Overview and concepts*
- [38] ISO/IEC/TR 29181-5, *Information technology — Future Network — Problem statement and requirements — Part 5: Security*
- [39] ISO/IEC 30182, *Smart city concept model — Guidance for establishing a model for data interoperability*
- [40] BSI, City Data Report, 2015. <https://www.bsigroup.com/en-GB/smart-cities/>
- [41] BSI, European Innovation Partnership for Smart Cities & Communities (EIP-SCC). EIP-SCC Urban Platform Management Framework. Enabling cities to maximize value from city data. Ver 03 October 2016. https://www.bsigroup.com/Sustainability/EIP_Mgmt_Framework.pdf
- [42] BSI. European Innovation Partnership for Smart Cities & Communities (EIP-SCC). Rethinking the city: using the power of data to address urban challenges and societal change A guide for city leaders, 2017. https://www.bsigroup.com/Sustainability/EIP_Leadership_Guide.pdf
- [43] Imperial College, London, D8.1: Common monitoring and evaluation framework (CMEF), Sharing Cities project funded by EU Horizon 2020, 2016.
- [44] Teesside University, D1.3 Data Management Plan, Demand Response in Blocks of Buildings (DR-BOB) project funded by EU Horizon 2020, 2016.
- [45] TNO, D2.1: Definition of data sets, CITYkeys project funded by EU Horizon 2020, 2016.
- [46] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- [47] Xianghao Nan, Combined Public Key (V8.0), *International Journal of Automation and Power Engineering* (IJAPE), 2014, 3:119 - 123
- [48] A Soft Key System and Its Implementation (China Patent: 201510028842.2).
- [49] A New Terminal Security Soft Key Management Method (China Patent: 201510690811.3)