

T/SZS

深圳市深圳标准促进会团体标准

T/SZS XXXXX—XXXX

防疫通行码参考架构与技术指南

Reference architecture and Technology guide of Health Code

征求意见稿

XXXX—XX—XX 发布

XXXX—XX—XX 实施

深圳市深圳标准促进会

发布

目 次

前言 II

引言 III

1 范围 1

2 术语、定义与缩略语 1

 2.1 术语与定义 1

 2.2 缩略语 1

3 防疫通行码架构 1

 3.1 概述 1

 3.2 技术架构图 2

 3.3 防疫通行码适用场景 2

4 防疫通行码技术要求 2

 4.1 民众端功能要求 2

 4.2 民众端数据采集要求 3

 4.3 防控检测端功能要求 3

 4.4 防控检测端技术要求 3

 4.5 防控管理端功能要求 3

5 数据保护 4

 5.1 安全防护 4

 5.2 数据安全 4

 5.3 个人信息保护 4

参考文献 5

前 言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由深圳市标准技术研究院与深圳市腾讯计算机系统有限公司联合提出。

本标准由深圳市深圳标准促进会归口。

本标准主要起草单位：深圳市标准技术研究院、深圳市腾讯计算机系统有限公司。

本标准主要起草人：王丽娟、王永霞、滕一帆、王刚、邓凯、罗志伟、赵亮。

引 言

在发生社会重大卫生事件的情况下，全国各地对应用新一代信息技术服务社会抗击疫情、服务企业复工复产具有急迫的需求，相应地也存在技术能力薄弱、多头重复建设、区域协同障碍、响应速度缓慢等问题。

基于互联网企业在本次疫情防控中，针对多地需求推出的“防疫通行码”技术，即通过利用数据互通和业务协同提升社会治理能力，推动应用防疫通行码技术，有效支撑基层疫情防控和社会治理，帮助众多企业和群众解决个人申报、企业申报、学校申报、社区申报、交通申报等多场景下采集数据标准不一致，采集数据不可用的问题；同时，满足社区，办公大楼，交通卡口，机场火车站等不同场景下非接触式安全授卡，通过手机亮码快速通行的需求，实现疫情防控和复工复产“两手都要硬”，特编制本标准。

防疫通行码参考架构与技术指南

1 范围

本标准规定了防疫通行码的架构、技术要求以及数据保护等内容。

本标准适用于民众通过手机小程序，填报一次“个人防疫状况”获得“防疫通行码”，凭借防疫通行码进出多种公众场所，如社区、办公口、交通卡口、机场火车站等，实现不同场景下的快速查验需求。

2 术语、定义与缩略语

2.1 术语与定义

下列术语与定义适用于本标准。

2.1.1

防疫通行码 Antiepidemic Pass Code

民众通过手机小程序在线申领，可作为进出社区、办公大楼、交通卡口、机场火车站等不同场景的通行凭证，且通过非接触式安全授卡的二维码。

2.1.2

架构 architecture

通过系统元素、元素间的关系，以及系统设计和进化原则体现出来的一个系统在其环境中的基本概念或属性。

[ISO/IEC/IEEE 42010:2011]

2.2 缩略语

3 防疫通行码架构

3.1 概述

防疫通行码，在应对社会重大影响事件，构建应急期间的个人防疫身份证“防疫通行码”统一标准，规范社区围合式管理以及路网卡口的通行监管，解决个人/企业员工防疫数据采集、管理问题。

根据角色配置不同职责权限，同时解决不同角色的数据采集和验证需求：

- a) 民众：疫情防控中，针对不同场景，定义为不同名称，如市民、村民、学生、企业员工等；
- b) 防控检测员：疫情防控一线工作人员，主要包含一线交警、网格员、公司管理者、学校管理员等；
- c) 防控管理员：疫情防控中各级防控管理责任员，如村委会、居委会、疾控部门等。

3.2 技术架构图

防疫通行码基于微信小程序，技术架构图见图 1。

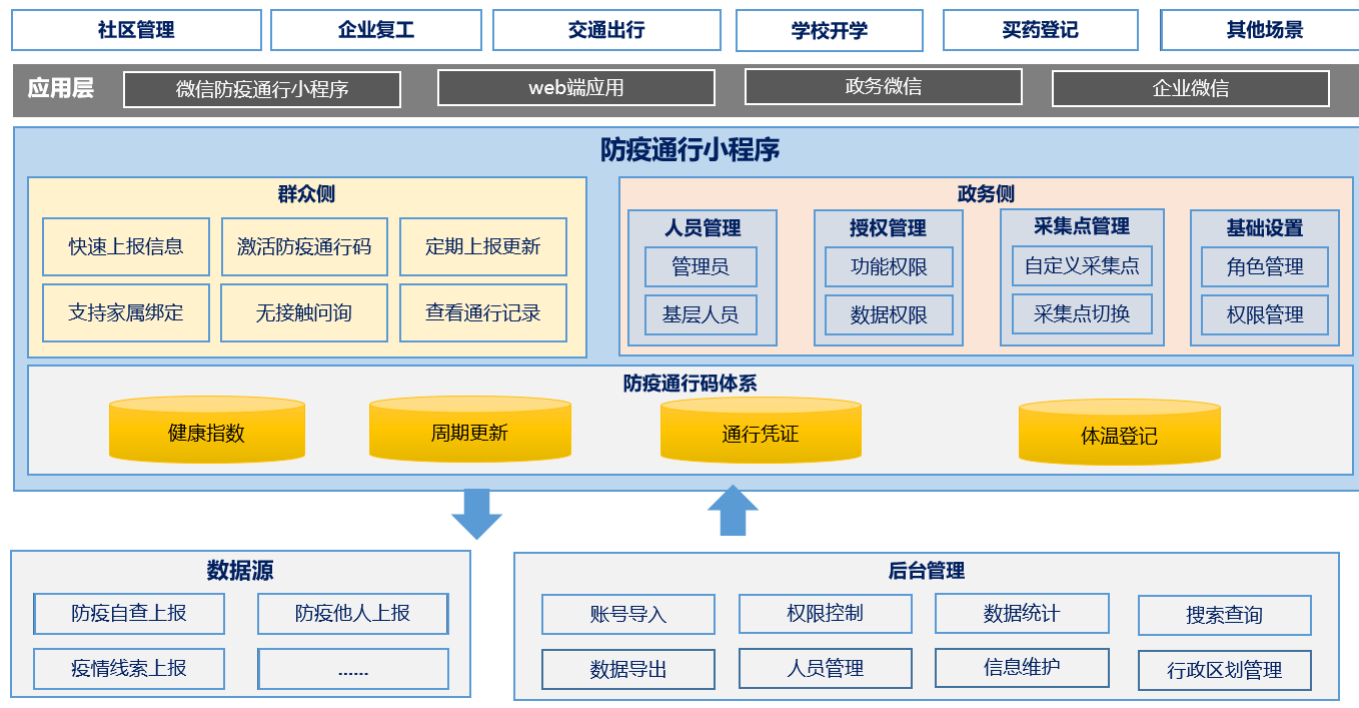


图1 防疫通行码技术架构图

3.3 防疫通行码适用场景

通过手机小程序支持民众上报防疫数据，生成有效防疫通行码，并应支持定期上报刷新、家属绑定（解决老人儿童出行）等功能，在以下场景下使用：

——社区、私家车、货车类型

针对人数在 12 人以下的社区进出或交通工具进行通行申报，特点是通行人员相对熟悉，即使不熟悉也是人数不多的群组通行。

——大巴、中巴车、班车类型

针对人数在 12 人以上的大中巴客车，主要以班车为主（不含公交车），特点是乘客数量多，但车辆有特定班次规律的群组通行场景。

——高铁、动车、火车、飞机、轮渡

超大规模运输工具，但有固定且封闭的客运站，乘客仍以单人出入站台闸口为特点的单人通行场景，亮码核查即可通行。

4 防疫通行码技术要求

4.1 民众端功能要求

民终端功能要求包括以下内容：

- a) 码申领：应支持对自身防疫状况、他人防疫状况、通行信息采集上报，并通过防疫通行码申领发放，实现闭环管理；

- b) 家属（团体）绑定：应支持为他人申请防疫通行码或扫一扫分享功能，绑定家属（团体）健康码；
- c) 上报信息刷新：应支持通过设置防疫通行码的有效时间，定期更新防疫信息。

4.2 民众端数据采集要求

4.2.1 数据采集方式

民终端数据采集方式包括以下内容：

- a) 自主申报：由民众自主自行申报提交，或由关联人员予以申报，并依据实际情况对申报信息进行修改；
- b) 核验调整：经由检测点检测后，在检测端对异常数据进行调整上报。

4.2.2 数据采集类型

民终端数据采集类型包括以下内容：

- a) 基础信息：包括采集对象的姓名、身份证件、住址、人员性质等主要信息，若采集对象以组织为单元，还应记录组织基本信息；
- b) 防疫信息：包括采集对象的症状、就医、隔离观察、接触人信息、居住旅行史等主要信息；
- c) 通行信息：包括行程始终地、出行方式、座次、出行时间、车辆信息、司乘信息等主要信息；
- d) 其他管理信息：包括采集方式、采集时间、采集地点等主要信息。

4.3 防控检测端功能要求

防控检测端功能要求包括以下内容：

- a) 出行核验：通过扫描受检人员出示的防疫通行码，获取其基本防疫信息，并记录本次出行情况；
- b) 检测点管理：支持添加检测点或更换检测点操作。

4.4 防控检测端技术要求

4.4.1 应定义检测事件类型，包括但不限于：

- a) 公路卡点采集；
- b) 机场车站码头采集；
- c) 社区采集；
- d) 物业采集；
- e) 政府单位采集；
- f) 企业采集；
- g) 学校采集；
- h) 医院采集；
- i) 网格员核查采集；
- j) 系统对接；
- k) 其他采集。

4.4.2 应定义检测人员角色，包括但不限于管理员、网格员等。

4.4.3 应定义检测人员的个人信息，包括但不限于姓名、电话、所属工作单位等。

4.5 防控管理端功能要求

防控管理端功能要求包括以下内容：

- a) 核验防疫信息：核查民众端上报的通行信息，包括时间、采集点、体温、出行状态、其他备注信息等；
- b) 采集员的授权管理：支持多层级的数据采集员管理，由管理员授权管理采集员；
- c) 设置采集点：支持管理员按需添加、设置采集点信息；
- d) 统计分析：支持对采集、核验的防疫信息进行统计分析，辅助防控措施的调整与资源配置；
- e) 应对同一通行区域实行统一管理、统一防护，提高综合防护能力。

5 数据保护

应符合《网络安全法》要求，采取必要措施，对攻击、侵入和破坏政府网站的行为以及影响防疫通行码正常运行的意外事故进行防范，加强网络安全监测预警，确保其稳定、可靠、安全运行。

5.1 安全防护

部署必要的安全防护设备，应对病毒感染、恶意攻击、网页篡改和漏洞利用等风险，保障防疫通行码安全运行。安全防护措施包括：

- a) 部署的设备和软件应具备与访问需求相匹配的性能；
- b) 根据用户类别设置不同安全强度的鉴别机制，严格设定访问和操作权限；
- c) 应对用户的操作行为进行日志记录。

5.2 数据安全

应采取以下措施确保防疫通行码数据安全：

- a) 定期备份数据，提升容灾备份能力；
- b) 建立信息数据安全保护制度，收集、使用用户信息数据应当遵循合法、正当、必要的原则；
- c) 收集或掌握个人信息的机构要对个人信息的安全保护负责，采取严格的管理和技术防护措施，防止被窃取、被泄露。

5.3 个人信息保护

应采取以下措施确保防疫通行码满足个人信息保护要求：

- a) 应遵循国家标准《个人信息安全规范》，坚持最小范围原则，为疫情防控等类似用途收集的个人信息，不得用于其他用途；
- b) 任何单位和个人未经被收集者同意，不得公开姓名、年龄、身份证号码、电话号码、家庭住址等个人信息，因工作需要或因社会治理工作需要，且经过脱敏处理的除外；
- c) 应防止形成对特定地域人群的事实上歧视。

参 考 文 献

- [1] GB/T 32400-2015 信息技术 云计算 概览与词汇
 - [2] GB/T 35293-2017 信息技术 云计算 虚拟机管理通用要求
-