

防疫通行码参考架构与技术指南

Reference architecture and Technology guide of Anti-epidemic Pass Code

2020 - 03 - 06 发布

2020 - 03 - 06 实施

目 次

前言	II
引言	III
1 范围	1
2 规范性应用文件	1
3 术语和定义	1
4 防疫通行码架构	2
4.1 概述	2
4.2 技术架构图	2
4.3 防疫通行码适用场景	2
5 防疫通行码技术要求	3
5.1 民众端功能要求	3
5.2 民众端数据核验要求	3
5.3 防控检测端功能要求	3
5.4 防控检测端技术要求	3
5.5 防控管理端功能要求	4
6 数据保护	4
6.1 总体要求	4
6.2 安全防护	4
6.3 数据安全	4
6.4 个人信息保护	5
参考文献	6

前 言

本标准按照GB/T 1.1-2009给出的规则起草。

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。

本标准在深圳市政务服务数据管理局指导下,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:深圳市大数据资源管理中心、深圳市标准技术研究院、深圳市腾讯计算机系统有限公司、深圳市华傲数据技术有限公司、中兴通讯股份有限公司、深圳市铨顺宏科技有限公司、平安国际智慧城市科技股份有限公司、深圳市嘉德永丰开发科技股份有限公司。

本标准主要起草人:王耀文、杨枫、罗菁春、张卫清、武刚、朱玮、李士明、刘峰、林宇群、潘晓军、孙飞、韩晨、刘辉、苏圳龙、王丽娟、王永霞、李媛红、滕一帆、王刚、段胡胡、胡敏、董婷、邓凯、罗志伟、柳建村、赵亮、刘斌、蒋映捷、李军、张宇翔、周峰、马伟、李冬梅、黎俊茂、陈立、李祝兰、王岳明。

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2020春节期间爆发的“新冠肺炎”疫情，针对多地疫情防控管理的迫切需求，互联网企业适时推出了“防疫通行码”技术，通过利用数据互通和业务协同提升社会治理能力。为推动防疫通行码技术应用，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。

在应对重大公共卫生事件中，通过构建应急期间的个人防疫身份证“防疫通行码”，规范社区围合式管理以及路网卡口的通行监管方式，解决个人/企业员工防疫数据采集、管理问题。本标准为深圳市范围内各级组织实施防疫通行码提供指导，也为全国各地推行防疫通行码提供参考。

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。
本标准适用于防疫通行码的设计、开发、使用、维护等。

2 规范性应用文件

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 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 35273-2017 信息安全技术 个人信息安全规范

GB/T 35274-2017 信息安全技术 大数据服务安全能力要求

全国一体化在线政务服务平台 防疫健康信息码服务接口

3 术语和定义

下列术语和定义适用于本标准。

3.1

防疫通行码 Anti-epidemic Pass Code

民众通过移动设备在线申领，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。

3.2

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]

3.3

亮码 Code Production

民众通过移动设备访问防疫通行码平台，终端屏幕显示防疫通行码的过程

3.4

扫码 Code Scan

核验人员通过移动设备登录防疫通行码平台，使用“扫一扫”功能扫描民众出示防疫通行码的过程。

4 防疫通行码架构

4.1 概述

防疫通行码根据不同角色配置不同职责权限，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、物业安防人员等；
- c) 防控管理员：疫情防控中各级防控管理责任人员，如村委会、居委会、疾控部门、社区和街道、医疗卫生、公安等防疫相关工作人员。

4.2 技术架构图

防疫通行码技术架构见图 1。本标准防疫通行码与《全国一体化在线政务服务平台 防疫健康信息码服务接口》标准进行对接，实现与国家平台防疫健康信息码的互信互认。

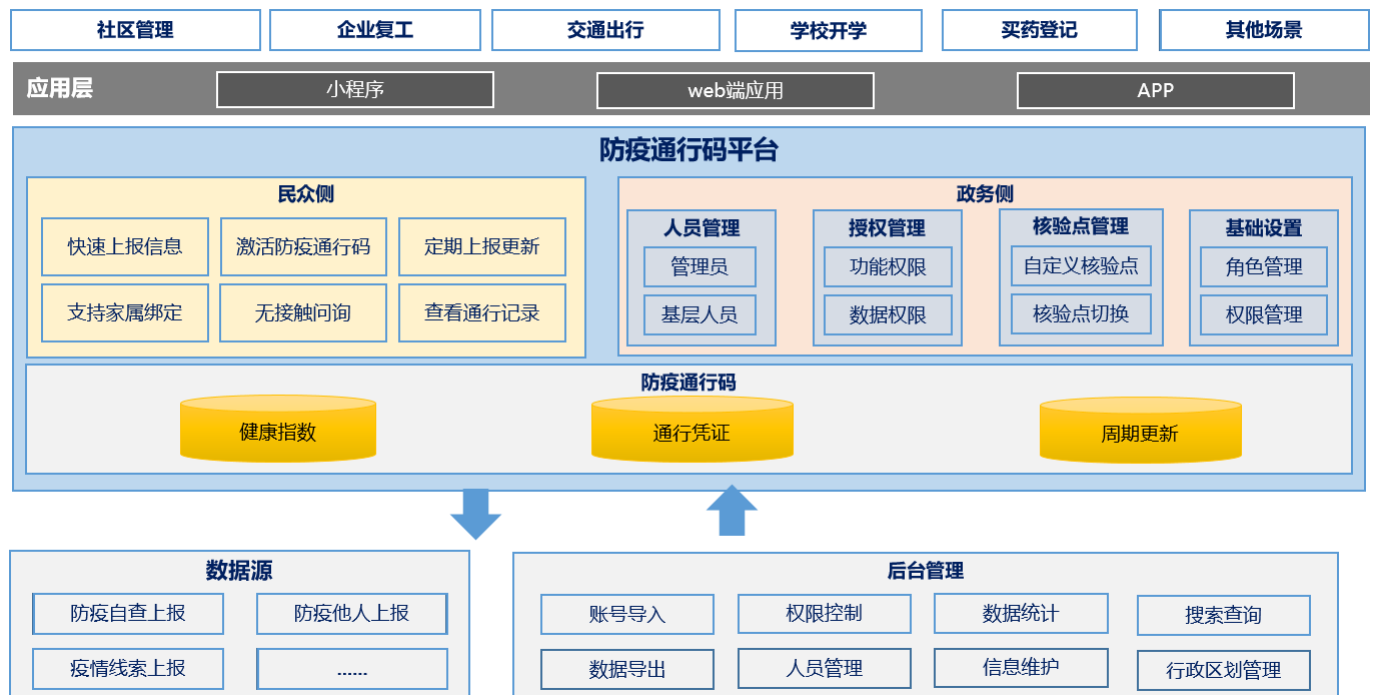


图1 防疫通行码技术架构图

4.3 防疫通行码适用场景

民众通过手机等移动设备，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。

在以下场景下使用：

——小区、城中村

针对小区和城中村等居住出行场景，通过亮码、扫码，作为出入居住地的电子凭证。

——交通卡口

针对城市交通卡口的车辆核查，通过亮码、扫码，作为进入城市的申报电子凭证。

——公交场景

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，可亮码备查提高通行效率。

——办公大楼、工厂、学校、商场、酒店等

人群密集场所，有固定且封闭的出入口，以单人出入为特点的通行场景，可亮码备查提高通行效率

5 防疫通行码技术要求

5.1 民众端功能要求

民众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) 防疫通行码应展示申领人员的姓名，健康状态等基本信息；
- d) 有效期管理：应支持通过设置防疫通行码的有效时间，申报更新防疫信息后重新产生防疫通行码。

5.2 民众端数据核验要求

5.2.1 数据核验方式

民众端数据采集方式包括以下内容：

- a) 自主申报：由民众自主申报提交；老人、小孩等缺乏自主申报能力的民众，可由家人代为申报；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。

5.2.2 核验数据类型

民众端核验数据类型包括以下内容：

- a) 基础信息：包括姓名、身份证件、地址、人员性质（如疑似患者密切接触史，常驻地之外的旅游居住史）等主要信息，若核验对象以组织为单元，还应记录组织基本信息；
- b) 防疫信息：包括症状（如发烧、咳嗽）、就医、隔离观察、接触人信息、疫区旅行史等主要信息；
- 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：包括核验人员、核验方式、核验时间、核验地点等主要信息。

5.3 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；并规定防控检测员的权限，明确可获取人员基本防疫信息的范围。
- b) 核验点管理：支持添加核验点或更换核验点操作。

5.4 防控检测端技术要求

5.4.1 应定义核验事件类型，包括但不限于：

- a) 公路卡点核验；
- b) 机场车站码头核验；
- c) 社区核验；
- d) 物业核验；
- e) 商场核验；
- f) 公园核验；
- g) 政府单位核验；
- h) 企业核验；
- i) 学校核验；
- j) 医院核验；
- k) 网格员核查核验；
- l) 系统对接；
- m) 其他核验。

5.4.2 应定义核验人员角色和个人信息，角色包括但不限于管理员、网格员等；个人信息包括但不限于姓名、电话、所属工作单位等。

5.5 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) 核验民众端上报的通行信息，包括时间、核验点、体温、出行状态、其他备注信息等；
- b) 支持多层级的核验人员管理，由管理员授权管理核验人员；
- c) 支持管理员按需添加、设置核验点信息；
- d) 支持对核验的防疫信息进行统计分析、疫情预警，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；
- f) 支持亮码、扫码运算，并面向各政府部门提供的数据共享外用

6 数据保护

6.1 总体要求

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。

6.2 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。
- d) 系统平台应符合 GB/T 22239-2019 中三级以上等级保护的要求。

6.3 数据安全

应采取以下措施确保防疫通行码数据安全：

- a) 应遵循 GB/T 35274-2017 建立数据安全保护制度，实施必要的数据安全技术措施；

- b) 定期备份数据，提升容灾备份能力；
- 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。

6.4 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 GB/T 35273-2017 的要求，收集、使用用户个人信息应当遵循合法、正当、必要的原则，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) 应采取适当措施对个人敏感信息进行了保护，防止因使用颜色等标识防疫通行码，形成对特定地域或特点人群的歧视。

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
 - [3] ISO/IEC/IEEE 42010:2011 Systems and software engineering — Recommended practice for architectural description of software-intensive systems
 - [4] GB/T 35274-2017 信息安全技术 大数据服务安全能力要求
 - [5] GB/T 35273-2017 信息安全技术 个人信息安全规范
-