ICS 33.050
CCS M 30

团　体　标　准

T/TAF 144—2023

数字政务服务快应用技术要求

Technical requirements for quick application of digital government services

2023-02-08 发布　　2023-02-08 实施

电信终端产业协会　发布

目　　次

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专利的责任。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、OPPO 广东移动通信有限公司、维沃移动通信有限公司、华为终端有限公司、小米通讯技术有限公司、亚信科技（成都）有限公司。

本文件主要起草人：杨正军、张宇鹏、陈婉莹、戈志勇、苏兆飞、张迎春、程鑫、高立发、刘家玮、谢斌锋、庄志强、刘鸣、赵驰、王晓航。

引　言

随着互联网技术的日趋成熟，利用新一代信息技术构建数字政府，推动政府部门的数字化改革成为新型政府的工作重点。数字政府是以互联网为基础，以新一代信息技术为支撑，以数据为关键要素的一种新型政府运作模式，利用数据驱动重塑政府职能，实现用数据决策、用数据服务、用数据创新的治理新模式。

2021年国务院办公厅印发《全国一体化政务服务平台移动端建设指南》，就进一步加强和规范全国一体化政务服务平台移动端建设，促进各地区各部门政务服务平台移动端标准化、规范化建设和互联互通，推动更多政务服务事项网上办、掌上办作出部署。快应用是移动端的重要组成部分，通过近几年的发展，已初具生态规模和用户规模，具有原生体验、即点即用等特性。2020年11月18日，国家政务服务平台快应用正式上线运行，是快应用服务于数字政府的成功案例，接入功能日趋丰富、注册人数日渐增长，实现了从“人找服务”到“服务找人”。

随着数字政府建设对移动端的重视以及数字政务服务对于快应用端建设需求的增加，亟需制定标准来规范政务类快应用的设计、开发、检测、运维、安全等技术要求，提高政务类快应用的服务质量，解决移动端管理分散、标准规范不统一、数据共享不充分、技术支撑和安全保障体系不完备等突出问题，推动我国数字政务服务移动端建设的高质量发展。

数字政务服务快应用技术要求

1 范围

本文件规定了数字政务服务快应用的技术架构，提出数字政务服务快应用在前端设计、接口开发、服务检测、云服务、上架部署、系统运维等方面的技术要求和管理要求。

本文件适用于政务类快应用的开发、运行、运维等项目实施，其他类快应用或小程序也可参考使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 信息安全技术网络安全等级保护基本要求

GB/Z 24294-2009 信息安全技术基于互联网电子政务信息安全实施指南

GB/T 31072-2014 科技平台统一身份认证

GB/T 35273-2020 信息安全技术个人信息安全规范

ZWFWC 0104-2018 国家政务服务平台移动端界面视觉要求

ZWFWC 0111-2018 国家政务服务平台统一身份认证系统身份认证技术要求

ZWFWC 0113-2018 国家政务服务平台统一信任服务平台接口要求

ZWFWC 0131-2018 国家政务服务平台统一身份认证隐私保护要求

3 术语和定义

GB/T 22239、GB/Z 24294-2009、GB/T 31072-2014、GB/T 32918、GB/T 35273-2020、ZWFWC 0111-2018界定的以及下列术语和定义适用于本文件。

3.1

快应用 quick application

基于硬件平台，用户无需下载安装、即点即用、原生的应用形态。

3.2

数字政务服务 digital government services

由政府部门为自然人、法人和其他组织提供各类网上政务服务。

3.3

私有云 private cloud

云服务仅被一个云服务客户使用，且资源被该云服务客户控制的一类云部署模型。

3.4

政务云 government cloud

运用云计算技术，统筹利用机房资源、计算资源、存储资源、网络资源、信息资源、应用支撑等资源，发挥云计算虚拟化、高可靠性、通用性、高可扩展性以及快速、按需、弹性的服务等特征，为各政务部门构建提供基础设施、支撑软件、应用系统、信息资源、运行保障和信息安全等服务的综合性云服务平台。

4 缩略语

APP：应用程序（Application）
CA：证书颁发机构（Certificate Authority）
CPU：中央处理器（Central Processing Unit）
H5：超文本标记语言第5版（Hyper Text Markup Language 5）
HTTP：超文本传输协议（Hyper Text Transfer Protocol）
HTTPS:基于安全通道的超文本传输协议(HyperText Transfer Protocol over Secure Socket Layer)
JAR：一种软件包文件格式（Java Archive）
JS：即时编译型的编程语言（JavaScript）
RPK：快应用应用程序包（Rapid Packages）
TCP：传输控制协议（Transmission Control Protocol）
TLS：传输层安全性协议（Transport Layer Security）
URL：统一资源定位器（Uniform Resource Locator）
UTF-8：可变长度字符编码（Unicode Transformation Format-8）

5 数字政务服务快应用概述

5.1 快应用概述

快应用是通过调用终端设备级和系统级能力实现的免安装、服务直达的一种应用形态。作为移动互联网新型应用形态，快应用与操作系统深度整合，具有免下载、免安装、一键触达、易于留存、原生体验、互联互通、无版本碎片等特点，能够让消费者体验到“秒开”。特别是在5G网络环境下，利用快应用形式来实现各种互联网服务，与手机系统层各入口相结合，极大地推动了5G的应用创新。

政务快应用是快应用在数字政务中的场景应用。政务类服务“低频、刚需、发展”的服务特性，与快应用“即点即用、原生体验、原子化服务、灵活高效触达用户”的特点相契合。

5.2 数字政务服务快应用技术架构

数字政务服务快应用架构如图1所示。

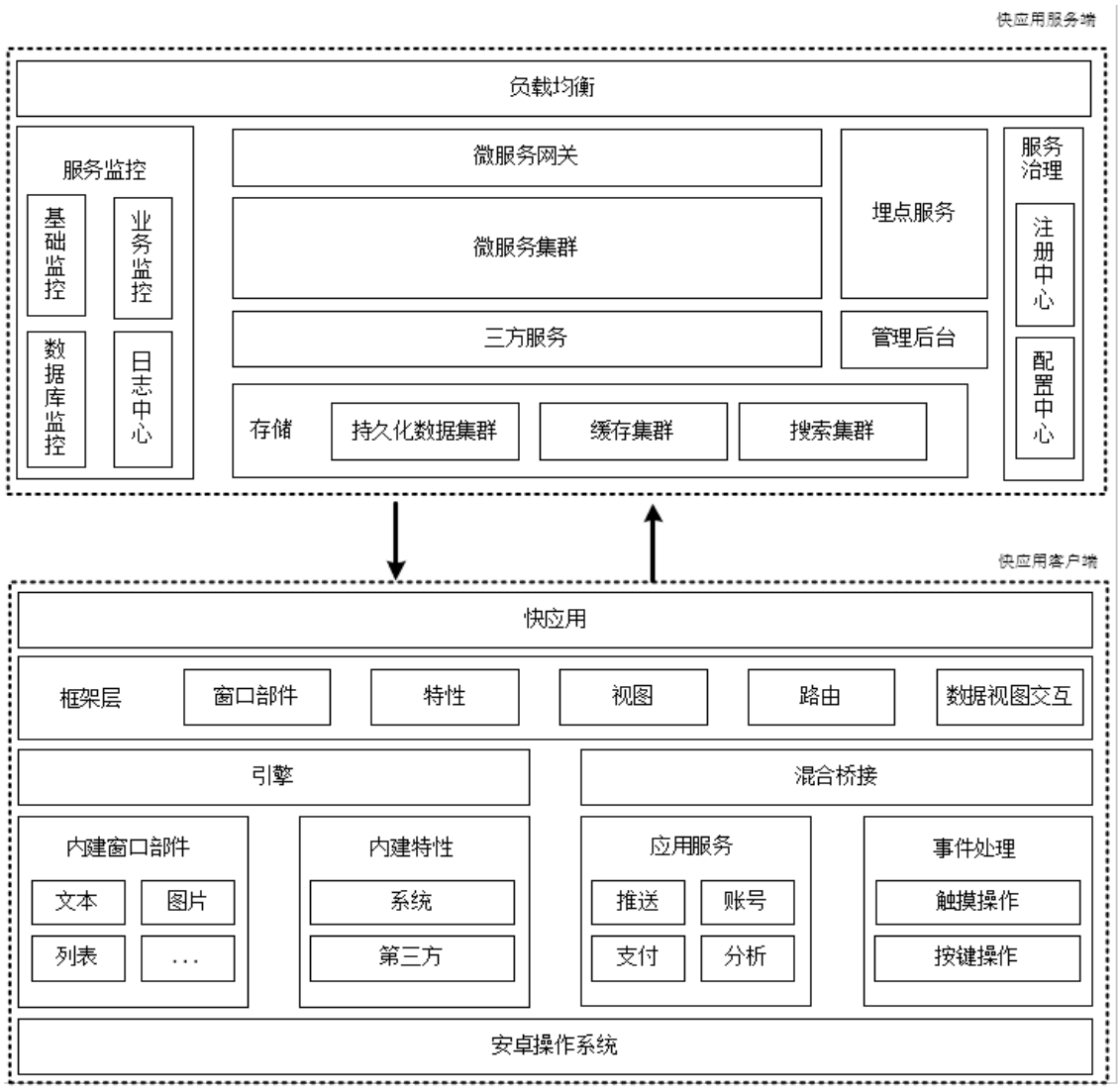

图1　数字政务服务快应用技术架构

数字政务服务快应用架构由服务端和客户端组成，具体如下：

a)　客户端：

1)　快应用：层应用，各类快应用服务；

2)　框架层：提供一般常见框架的基本能力建设，如：数据视图交互、视图、路由和组件等；

3)　引擎层：分为 JavaScript 引擎和渲染引擎，JavaScript 引擎负责开发者 JS 代码的执行，渲染引擎负责原生组件的布局计算；

4)　混合桥接层：负责连接框架层和应用层，将底层应用能力提供给快应用框架层；

5)　内建窗口部件：即各类 UI 组件库，如：文本、图片、列表等；

6)　内建特性：提供系统和三方服务的原生接口，如：网络、设备、二维码、加密等；

7)　应用服务：提供系统能力与第三方服务，如：推送、账号、微信支付等；

8)　事件处理：设备交互事件处理，如：屏幕触摸、按键操作等；

9)　安卓操作系统：提供最底层的系统服务。

b)　服务端：

1) 负载均衡：由于服务接口是分布式部署，所以当客户端请求服务端接口时，可将请求均匀分布在各机器节点，使得每部接口节点负载均衡；
2) 服务监控：含有基础监控、业务监控、数据库监控和日志中心，统一对服务进行监控告警处理；
3) 微服务网关：将客户端请求路由转发到服务端；
4) 微服务集群：多个应用功能服务组成的服务集群；
5) 三方服务：主要由数字政务其他支撑功能提供接入方式来接入规划服务；
6) 埋点服务：用于记录行为过程及操作路径，用于数据分析和用户体验优化；
7) 管理后台：通过可视化管理后台进行维护，控制首页服务上下架以及静态资源的处理；
8) 服务治理：注册中心负责各个服务的管理和发现，通过统一的路由分发请求；配置中心使代码与配置解耦，将服务配置项统一管理；
9) 存储：持久化数据集群，缓存集群，搜索集群等，统一对项目数据进行处理和维护。

5.3 数字政务服务快应用业务流程

5.3.1 业务流程架构

数字政务服务快应用业务流程如图2所示：

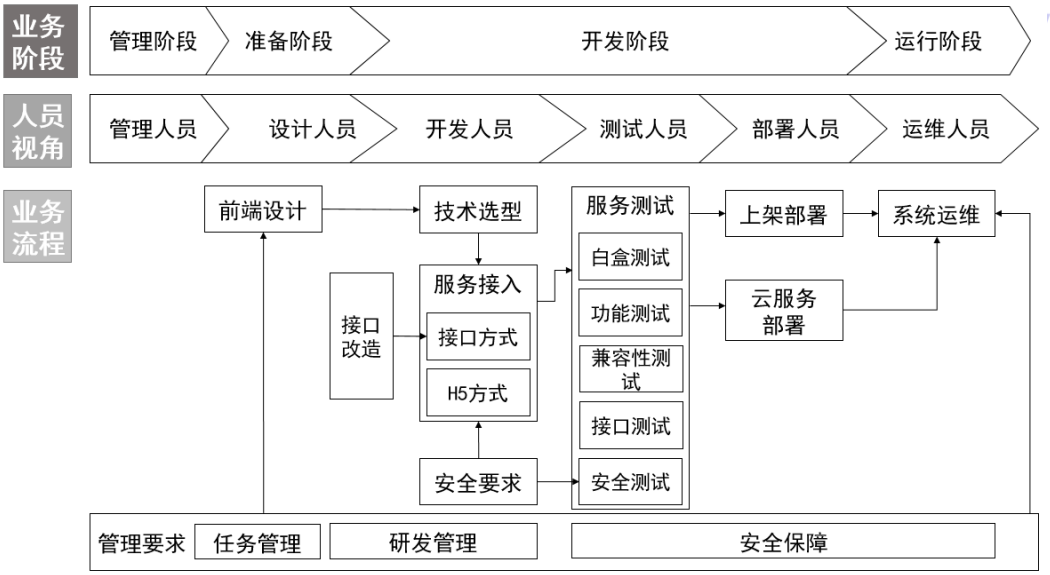

图2 数字政务服务快应用业务流程

数字政务服务快应用业务流程分为四个阶段：管理阶段、准备阶段、开发阶段、运行阶段。

5.3.2 管理阶段

管理阶段主要由管理人员对数字政务服务快应用业务进行各阶段管理应遵循的规范要求，如任务管理、研发管理、安全保障等。

5.3.3 准备阶段

准备阶段主要由设计人员在业务准备阶段根据业务需求进行前端设计。

5.3.4 开发阶段

业务开发阶段主要由开发人员、测试人员、部署人员开展技术选型、服务接入、服务测试、上架部署等工作。

5.3.5 运行阶段

运行阶段主要由运维人员开展系统运维、数据备份、安全加固与日常巡检等工作。

6 数字政务服务快应用技术要求

6.1 前端设计技术要求

数字政务服务快应用界面设计应从自然人、法人和其他组织使用便利角度出发，减少用户操作，方便用户浏览和查询相关内容，具体要求如下：

a) 应符合移动设备的交互方式，应兼容当前主流移动设备的屏幕尺寸与分辨率；
b) 弹出窗口、漂浮窗口确需使用时，不应使用多个窗口，且窗口应提供关闭按钮；
c) 如有政务服务门户网站或 APP 端，整体色调应与门户网站或 APP 端保持一致，如主色、辅助色、图标整体设计风格等，具体参考 ZWFWC 0104-2018 要求，改版或调整时不应改动；
d) 数字政务服务快应用的界面视觉设计应支持残障人士的无障碍浏览。

6.2 程序开发技术要求

6.2.1 技术选型

数字政务服务快应用在开发前应进行技术选型，选型项目应包括以下内容：

——虚拟机；
——Web 框架；
——数据交换格式；
——配置中心；
——注册中心；
——熔断限流重试；
——数据库连接；
——监控；
——日志分析；
——http 调用；
——数据库；
——消息中间件。

6.2.2 接口开发技术要求

6.2.2.1 服务接口改造技术要求

以接口形式提供的政务服务，接口改造时，应在权限管理和防篡改方便进行处理，具体包括：

a) 服务接口权限分配：针对快应用系统中用户的未登入、登入（实名）、登入+人脸验证（业务标示）三种状态，服务接口使用时应将权限分配为：不需要登入、需要登入（实名）、需要登入（实名）+ 人脸验证；
b) 服务接口防篡改：涉及人员信息、查询结果等安全性要求严格的接口，应进行防篡改处理。

6.2.2.2 接口返回值格式要求

接口程序开发期间，应对接口响应码、用户提示信息、接口具体数据返回值格式提前设定，详细描述见表1，接口响应码定义列表示例见附录A。

表1　接口返回值格式描述

字段名	字段类型	是否必须	字段描述
code	Integer	Y	接口响应码
msg	String	N	用户提示信息，在必要时服务器返回给用户的提示，需要前端展示给用户
data	Object	N	接口具体的数据，结构取决于当前业务接口

6.2.3　H5 开发技术要求

以H5形式提供的政务服务，需要请求URL对接服务功能，对请求URL开发时应满足以下要求：

a）　请求URL对接服务时，URL中字母应全部为小写；

b）　如果有单词拼接时，应使用中划线‘-’，不应使用下划线‘_’；

c）　资源应采用资源名词的复数形式。

6.2.4　服务稳定性保障要求

服务开发完成后应保障上线后的运行稳定，服务上线前与上线后应至少满足以下要求：

a）　同一服务应多实例部署，并由注册中心统一管理，均衡调配；

b）　应对上线服务具备限流、熔断、降级机制，防止流量超出；

c）　服务上线前，应进行容量规划与全链路压测；

d）　服务上线前应评估接口性能，设置超时时间和重试次数。

6.3　安全技术要求

6.3.1　信息安全要求

6.3.1.1　基础要求

数字政务服务快应用信息安全基础要求包括：

a）　应开展网络安全等级保护定级备案工作，具体要求见 GB/T 22239；

b）　使用的密码技术和产品应符合国家或行业标准，并符合相应的法律法规要求。

6.3.1.2　身份认证

数字政务服务快应用进行身份认证时，应参照ZWFW C0111-2018进行技术设计。

6.3.1.3　快应用开发

数字政务服务快应用开发，应满足以下安全要求：

a）　代码与界面中不应含有黄赌毒、暴力、宗教、政治、人权等敏感词汇、敏感图片或其他形式内容；

b）　应进行安全防护，如设置组件最小化权限、删除测试信息等；

c）　应具备恶意攻击防范能力，能抵御 APT 攻击、间谍软件等攻击等；

d）　应具备防篡改能力，保证信息在接入过程中不被非法获取及篡改；

e）　应保证数字政务服务快应用不含有国家信息安全漏洞库（CNNVD）、国家信息安全漏洞共享平台（CNVD）等漏洞库 6 个月前公布的高危漏洞。

6.3.2 数据安全要求

6.3.2.1 基础要求

数字政务服务快应用数据安全基础要求包括：

a) 涉及个人信息的应符合 GB/T 35273-2020 要求，其中用于政务服务身份认证的数据还应符合 ZWFW C0131-2018 要求；
b) 数据收集和使用应符合业务需要，明确责权，贯彻知情同意原则；
c) 登录账号、姓名、证件编号、手机号、户籍地址、工作单位等敏感个人信息收集应坚持最小化原则；
d) 日志打印时，应脱敏打印姓名、身份证号、密钥等敏感数据。

6.3.2.2 数据传输

对于敏感个人信息传输，应满足以下内容：

a) 客户端和服务器的通信应只能通过 HTTPS 的方式传输，且应整体采用 HTTPS（TLS1.2 以上），客户端对服务器单向认证的方案；
b) 宜采用公钥密码算法并且获得信任的 CA 机构证书（或者数字政务服务提供域名、证书）；
c) 应集成 CA 机构根证书，验证手机厂商证书合法性，完成服务端认证；
d) 应采用密码技术保证数据传输的保密性和完整性，如：数字信封等。

6.3.2.3 数据存储

对于敏感个人信息存储，要求做到以下内容：

a) 对称加密算法宜使用 SM4；
b) 敏感个人信息在服务端存储时，应采用密钥分层管理机制来管理密钥；
c) 根密钥的管理宜采用基于密钥组件的根密钥管理方案，即组成根密钥的密钥组件分散存储在系统中，根密钥仅在需要时由密钥组件动态生成；
d) 对于不需要还原且唯一标识的数据宜使用杂凑算法进行计算，并对摘要数据进行 Base64_URLSafe 编码。

注：针对以上所有用到加密、摘要的字段，如果原文是字符串，应将字符串显式地按照 utf-8 编码方式转换成字节数组，如果是解密后的数据还原成字符串，应将解密后的字节数组按照 utf-8 编码方式转换成字符串。

6.3.3 安全管理要求

数字政务服务快应用安全管理要求包括：

a) 重要岗位人员应签署岗位安全保密协议，防止重要信息外泄；
b) 应制定密码安全管理制度及操作规范；
c) 应建立安全监测机制，预防和应对安全事件的发生，并制定应急预案；
d) 每年至少开展一次第三方安全评估工作，包括资产识别、威胁识别、脆弱性识别等方面。

6.4 服务检测技术要求

6.4.1 测试范围

数字政务服务快应用测试范围应包括：白盒测试、功能测试、兼容性测试、接口测试、安全测试等。

6.4.2 白盒测试

白盒测试的要求如下：

a) 应确保手头的原型图与效果图为当前最新版本；
b) 应确保制定的原型图、效果图与服务一致；
c) 应根据效果图检查服务界面；
d) 应预先考虑正式环境中可能出现的数据类型。

6.4.3 功能测试

功能测试的要求如下：

a) 应进行 UI 测试，保障界面显示正确；
b) 应能够探索遍历到用户文档中写明的主要功能，并且所有的功能都按照设计的方式正确运行；
c) 应对各个功能点进行正常场景测试和异常场景测试；
d) 应保证功能测试用例 100%覆盖。

6.4.4 兼容性测试

兼容性测试的要求如下：

a) 应确保软件在不同终端上都能正常使用；
b) 应确保软件在同一终端不同系统软件版本上可正常使用；
c) 应确认新旧版本的在功能层面的兼容性；
d) 应确保软件在不同引擎版本上正常使用。

6.4.5 接口测试

接口测试的重点是要检查数据的交换、传递和控制管理过程，以及系统间的相互逻辑依赖关系等，具体要求为：

a) 应对接口在业务功能正常场景和异常场景下数据交换、传递进行测试；
b) 应对接口输入输出边界测试，测试项应包括：参数必填非必填、参数排序、参数个数、参数类型、参数长度、参数包含特殊字符等；
c) 应对接口安全性、敏感信息加密、权限控制等过程管理进行测试。

6.4.6 安全测试

应制定安全测试方案，测试内容应覆盖本文件5.3章内容。

6.5 上架部署技术要求

6.5.1 服务部署前检查

服务部署前应在测试环境上先进行验证。

6.5.2 生产环境部署要求

测试环境验证后，可在生产环境上进行服务部署，部署时需要满足以下要求：

a) 应使用标准化的持续构建系统生成 jar 包；
b) 应区别老版本打新标签后再部署生产环境；
c) 部署前应检查线上配置文件，并与 jar 包一起打包。

6.5.3 部署完成后

服务部署在生产环境后，应完成以下要求：

a） 应对 rpk、服务端、服务功能进行验证；

b） 应对服务上线时间、内容进行登记。

6.6 云服务技术要求

数字政务服务快应用云服务的要求如下：

a） 应将云服务部署在指定的政务云上，且政务云应为私有云；

b） 应区分测试环境与生产环境；

c） 应对生产环境进行各项安全防护，确保政务云服务器安全稳定。

6.7 系统运维技术要求

6.7.1 基础要求

数字政务服务快应用系统运维工作的基础要求如下：

a） 应进行每日巡检，密切注意监控数据，保障系统正常平稳运行；

b） 数据库应每天至少备份一次；

c） 应定期对服务器进行安全加固；

d） 应根据服务器漏洞报告及处理建议及时进行补丁安装及软件版本升级；

e） 若监控出现告警情况，应提取相关服务日志，定位故障问题，并及时恢复服务（重启、扩容、替换服务器等）；

f） 解决告警情况后，应对故障进行复盘，准确找到问题根源，并对此问题进行优化操作。

6.7.2 运维监控

数字政务服务快应用系统运维监控包括但不限于基础运维监控、中间件监控、数据库监控、关键业务监控等，各项监控内容包括：

a） 基础运维监控应包括：IO 使用率、CPU 负载、内存占用、网卡接收发送量、TCP 连接、硬盘使用率等基础的资源监控；

b） 中间件监控应包括：对象数、连接数、命中率、碎片率等；

c） 数据库监控应包括：主从延迟、慢查询等。

d） 关键业务的实时监控应包括：请求数、成功数、失败数、平均耗时、最大耗时等； 并且要求对关键路径的关键日志进行监控，及时通过日志感知异常情况。

6.7.3 接口巡检

数字政务服务快应用应对后端接口进行运维巡检，要求如下：

a） 应接入服务主要接口；

b） 应在生产环境下实现自动化巡检；

c） 应满足新服务首月30分钟一次；服务稳定后一天两次的巡检周期。

7 管理要求

7.1 任务管理

数字政务快应用服务制作任务管理应满足以下要求：

a） 任务下发物料应完整；

b） 页面设计图应清晰；
c） 功能需求应明确；
d） 服务流程图应明晰。

7.2 研发管理

服务研发期间应严格遵守物料内容，不得随意私下更改。

7.3 安全保障

项目管理人员应对数字政务服务快应用安全高度重视，要求满足以下内容：
a） 数字政务服务快应用上线前，应覆盖本文件 5.4 章服务检测技术要求；
b） 应每季度对数字政务服务快应用所有服务器进行基线测试和漏洞扫描测试；
c） 每季度应盘点系统资源，应做到资产清晰可追溯、可查找。

附 录 A
（资料性）
接口响应码定义列表示例

接口响应码定义如表A.1所示：

表 A.1 接口响应码定义列表

10000(系统内部错误)	
code	类型
0	返回成功
10000	系统业务繁忙
10019	系统业务繁忙，建议稍后重试
10002	用户登录已过期（25 分钟账号登录过期，前端使用加密信息自动登录）
10003	已经登入，未验证人脸
10004	账号授权过期
10005	授权码无效
10006	参数 token 不存在
10007	数字政务 token 已过期
10008	用户未授权
10009	授权获取为空
10010	用户信息获取为空
10011	Openid 获取为空
10012	设备 ID 不一致，请重新登录
10013	用户已经存在绑定关系
10014	身份证与姓名不一致
10015	未绑定手机号
10016	身份证姓名校验失败
10017	用户登录已过期；用户 session30 天过期；需要用户手动输入登录
10022	未查询到数据
10023	用户已解绑数字政务服务账号
10024	手机号未授权
10025	人脸校验失败
10026	年龄不在查询范围，请使用’帮他人领取防疫健康信息码’
10027	认证失败次数超限，请稍后再试
10000~11000	通用错误码
11001~13000	A 类业务错误码
13001~15000	B 类业务错误码
15001~17000	C 类业务错误码
17001~19000	D 类业务错误码
17001	行程信息核验失败
17002	二维码已失效或已过期
19001~19999	预留

表 A.1 接口响应码定义列表（续）

20000（客户端错误）	
code	类型
20000	参数错误
20001	服务器拒绝请求
20002	请求方法不支持
20003	参数不能为空
20004	参数解密失败
20404	404
30000（三方系统错误）	
code	类型
30000	第三方接口请求失败
30001	三方系统超时
30002	三方系统连接超时
30003	三方系统读取超时
30011	三方系统数据解析失败
30012	三方系统直接返回错误码提示系统异常
30013	返回非 200 响应码

电信终端产业协会团体标准

数字政务服务快应用技术要求

T/TAF 144—2023

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn