ICS 35.240.99
L 67

ZWFW

广 东 数 字 政 府 标 准 规 范

GDZW 0001.6-2019

粤省事移动政务服务平台
第 6 部分：安全规范

2019-8-9 发布　　2019-8-9 实施

广东省政务服务数据管理局　发布

目 次

前　言

GDZW 0001《粤省事移动政务服务平台》分为六个部分：

——第1部分：总体规范；

——第2部分：数据规范；

——第3部分：功能规范；

——第4部分：建设规范；

——第5部分：运营规范；

——第6部分：安全规范。

本部分为GDZW 0001的第6部分。

本部分按照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。

本部分由广东省政务服务数据管理局提出并归口。

粤省事移动政务服务平台 第6部分：安全规范

1 范围

本部分规定了广东省粤省事移动政务服务平台的安全总体要求、安全技术要求、安全和应急管理要求。

本部分适用于粤省事移动政务服务平台的安全建设和运营、广东省各部门和各级政府政务服务应用接入粤省事移动政务服务平台的安全管理。同时可作为广东省各级政府及部门其他移动政务服务平台安全建设和运营的参考。

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 信息安全技术 信息系统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

3 缩略语

API 应用程序编程接口（Application Programming Interface）

HTTPS 超文本传输安全协议（Hypertext Transfer Protocol Secure）

OCR 光学字符识别（Optical Character Recognition）

4 总体要求

粤省事移动政务服务平台的技术和管理应满足GB/T 22239的第三级基本要求。

5 安全技术要求

5.1 物理、网络和主机安全

粤省事移动政务服务平台的物理、网络和主机安全应由广东省“数字政府”政务云平台保障。除云平台提供的安全保障体系外，粤省事移动政务服务平台还应满足数据安全、应用安全的要求。

5.2 数据安全

5.2.1 数据安全保护

粤省事移动政务服务平台应通过安全、保密、访问控制等手段向任何个人或单位关键数据（或重要、敏感数据）提供隐私保护和数据安全保护。

粤省事小程序展示个人重要信息时，应进行数据脱敏后再展示，对个人隐私信息做好保护。系统仅允许用户查看自己的相关信息，并且在除了信息录入环节外的其他界面对数据做脱敏处理，不完整显示用户敏感数据。对于他人代办业务、由他人查询相关信息的情形，如通过机动车牌号码、发动机号码、车架号码查询交通违法时，系统应只显示违法的主干信息，不显示车主个人隐私数据。个人敏感信息判定按照GB/T 35273-2017。

5.2.2 数据存储安全设计

用户在办理业务时如需要使用到用户实名等信息，应提示用户进行授权，用户授权确认后，系统才可调用外部系统获取信息；业务办理完毕后，系统应在内存中清除用户实名等信息。

5.2.2.1 前端数据储存设计

前端对数据存储要求如下：

a) 跟业务相关的数据应使用手机运行内存存储，在小程序生命周期内有效；

b) 跟业务无关或者已经脱敏的数据按照需要可存于手机机身内存，应设置有效期。

5.2.2.2 后端数据储存设计

系统对用户上传的照片、用户信息的处理，应遵循按需获取、用后清除的原则；对用户的敏感信息，应遵循不保存、不落地原则。对用户拍照、个人信息、日志的储存应符合以下要求：

a)用户拍照上传文件

在办理各项民生服务业务过程中，用户对证件、车牌、银行卡等拍照并上传图片，图片上传完成后系统应清除内存中的照片数据。

b)用户填写个人信息

粤省事小程序提供用户存储个性化信息的设置功能，方便用户办理特定业务。用户通过此功能，可以设置保存个人的收件地址、电话号码、姓名、性别、户籍、生日、民族等；用户如选择自动通过后端系统获取的方式来填写，系统应提示用户进行授权，用户授权后，系统才可进行调用外部系统获取个人常用信息。

c)系统审计日志

应对用户身份信息脱敏后再进行日志记录。

5.2.2.3 支持数据序列化处理技术

数据应采用序列化处理技术进行数据结构序列化、反序列化，以实现高效的压缩、存储。

5.2.3 关键数据加密

应对重要、敏感或关键数据实行分级加密存储，支持字段级、记录级、文件级加密存储。系统对于用户关键数据，如用户的微信ID及用户身份证号码、姓名等关联信息，应在数据库中进行序列化、MD5等不可逆化防止泄漏用户关键数据。

5.2.4 数据访问日志记录

对于所有涉及到数据文件、数据库记录的操作均应有日志，对所有的数据库操作应设置有日志审计记录。数据库的更新操作应通过数据库事务日志记录，并传到专用的数据库日志服务器，防止数据库文件被破坏导致用户数据丢失或泄漏。

系统应记录用户访问系统、办理业务过程中的系统日志，供系统审计使用。系统应记录业务逻辑的关键路径以及出错信息，方便线上排错；如需记录用户身份信息，应对用户身份信息脱敏后再进行日志记录。

5.3 应用安全

5.3.1 身份鉴别

5.3.1.1 微信、小程序双重身份识别

应提供专用的登录控制模块对登录用户进行身份标识和鉴别：

a) 微信端。应提供用户名密码登录，防止被盗用。

b) 微信小程序。由于微信小程序支持实名验证，系统在使用过程中应校验当前小程序的用户与系

统注册登记用户身份是否一致，如不一致不能使用。

5.3.1.2 唯一身份标识

应提供用户身份唯一标识鉴别功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用。用户的唯一识别标识为身份证号码，系统应通过身份证号码检查用户的唯一性，确保用户信息不被冒用。对于已经注册的用户，当事人可凭身份证通过人脸识别方式认领，或通过联系后台人工验证身份方式认领。

5.3.1.3 登录失败控制

应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施。

a) 固定时间内对于某个客户端对服务的调用应具有次数限制，超出设定范围的将作为重点监控目标存在，并限制用户当天不可登录。对于多天多次登录用户纳入黑名单。
b) 为保证安全，系统应只允许同一时间同一用户在一个终端登录，当用户登录一台终端后，其他登录状态终端将自动退出，不能再办理业务也不能收到相关提醒通知以防止数据泄漏。

5.3.1.4 WEB 中间件加固

承载应用的WEB中间件应符合以下加固配置，防止因中间件漏洞导致的入侵：

a) WEB 中间件应在官网渠道下载，使用最新的稳定版本；
b) WEB 中间件在安装时不应引入不必要的模块；
c) WEB 中间件在运行中应符合以下要求：使用普通权限运行，删除 web 应用默认页面；配置策略设置不允许进行目录浏览，以防止系统敏感信息外泄。

5.3.1.5 数据库加固

支撑应用的后端数据库应符合以下加固配置，防止因数据库漏洞导致的入侵：

a) 数据库程序应在官网渠道下载，使用最新的稳定版本；
b) 数据库程序应配置以下帐号管理及认证授权策略：按照用户分配帐号，禁止不同用户间共享帐号；删除或锁定与数据库运行、维护等工作无关的账号；限制具备数据库超级管理员权限的用户远程登录；根据用户的业务需要，配置其所需的最小权限；
c) 连接数据库的用户口令长度应至少 8 位，并包括数字、小写字母、大写字母和特殊符号 4 类中至少 2 类；用户口令的有效期应小于 90 天；禁止使用系统自带的默认口令。

5.3.2 访问控制

用户在小程序中的访问控制级别定义为：

a) 1 级登录：即游客态，无需任何登录或授权的用户登录态；
b) 2 级登录：即微信授权，用户同意授权小程序获取微信的公开信息，包括微信昵称、头像；
c) 3 级登录：即实名登录，使用微信支付实名认证，已绑定银行卡的用户需输入支付密码确认本人身份，未绑卡的用户直接进入刷脸流程；
d) 4 级登录：即实人登录，使用微信刷脸认证流程。

在办理业务过程中，不同业务对登录级别要求不同，需要更高安全等级时，应要求用户输入微信支付密码或微信刷脸认证以匹配登录级别。

5.3.3 采用安全传输协议

平台与第三方应用集成接口应采用HTTPS安全传输协议。第三方应用服务部署在互联网时，应提供HTTPS协议的接口，或提供内容加密的HTTP协议接口。平台应支持对传输链路加密，每个应用分配不同的密钥，支持对传输内容加密。第三方应用服务接口接入平台，应在响应头上带上响应签名。

5.3.4 请求合法性保障

5.3.4.1 基于签名算法验证

第三方应用与公共支撑平台的网关服务之间应约定一个TOKEN（通讯密码），所有由网关发出的请求都应在请求头中带上由这个TOKEN生成的签名，只有成功用签名算法计算并校验签名的请求才是有效的请求。

5.3.4.2 可扩展签名字段校验

公共支撑平台的网关服务可以扩展需要计算签名的字段，保证请求的合法性。

5.3.4.3 特定服务特性校验

公共支撑平台的网关服务应根据服务的访问特性，自动过滤非法特性请求。

6 安全管理要求

6.1 网络安全等级保护制度执行

运营方和接入方应根据《中华人民共和国网络安全法》等法律法规要求，严格执行网络安全等级保护制度，保障粤省事移动政务服务平台和业务系统免受干扰、破坏；应加强内、外部人员管理，开展安全意识培训，防止数据泄露或者被窃取、篡改。

6.2 平台建设管理

6.2.1 平台安全测评

粤省事移动政务服务平台和业务系统在“数字政府”政务云平台上线前，运营方和接入方应按照《广东省电子政务云平台管理暂行办法》有关规定，开展第三方安全测评。

6.2.2 应用接入

各业务系统接入粤省事移动政务服务平台时，其接口应满足以下条件，包括但不限于：

a) 业务系统对接粤省事移动政务服务平台的接口目录，不应与原业务系统部署在同一个目录下，应单独建立新目录对接到粤省事移动政务服务平台（即绑定在智能网关的目录）；

b) 业务系统应严格按照网关开发文档开发，区分用户业务接口和后端业务接口，不应将后端业务接口发布到用户业务接口上；

c) 各个接口不应存在 SQL 注入漏洞，宜使用参数化查询；

d) 各个接口应对用户鉴权，禁止用户创建、更新、读取、删除其他用户的信息；

e) 文件上传模块应禁止任意文件上传，应通过白名单限制上传格式；

f) 敏感接口（如：短信接口、邮件接口）应做频率限制：60 秒一次，验证码长度应为 6 位，有效期 3 分钟；

g) 需验证码校验的事项，校验成功后应返回 token 值，并传递到下个页面接口再次校验 token 有效性；

h) 个人办理事项，不应从用户端获取用户身份，应从智能网关的请求的 header 头获取；

i) 业务系统返回个人信息类的数据时应对用户敏感信息进行掩码处理，不应返回明文；

j) 接入的事项应对业务系统合理配置错误页面（403、404、405、500、503、504 等），禁止泄露中间件错误页面；

k) 若无特殊需要，应使用 GET、POST 两种 http 方法。

6.2.3 应用测试

政务服务应用在粤省事移动政务服务平台上线前应进行安全测试，宜重点测试应用是否存在表 1 所述漏洞。

表 1 漏洞测试项目

编号	测试名称	漏洞级别	漏洞说明
STC-1	SQL 注入漏洞测试	高	SQL 注入攻击包括通过输入数据从客户端插入或“注入”SQL 查询到应用程序。
STC-2	XSS 漏洞测试	中	如果应用程序发送给浏览器的页面中包含用户提供的数据，而这些数据没有经过适当的验证或转义（escape），就会导致跨站脚本漏洞。
STC-3	CSRF 漏洞测试	中	用户以当前身份浏览到 flash 或者恶意网站时，JS/flash 可以迫使用户浏览器向任意 CGI 发起请求，此请求包含用户身份标识，CGI 如无限制则会以用户身份进行操作。
STC-4	文件上传漏洞测试	高	Web 应用程序在处理用户上传的文件时，没有判断文件的扩展名是否在允许的范围内，就把文件保存在服务器上，导致恶意用户可以上传任意文件，甚至上传脚本木马到 web 服务器上，直接控制 web 服务器。
STC-5	文件下载漏洞测试	高	处理用户请求下载文件时，允许用户提交任意文件路径，并把服务器上对应的文件直接发送给用户，这将造成任意文件下载威胁。
STC-6	命令执行漏洞测试	高	web 应用代码中，允许接收用户输入一段代码，之后在 web 应用服务器上执行这段代码，并返回给用户。
STC-7	URL 跳转漏洞测试	中	某些页面由于功能需要进行页面跳转，如果没有对跳转的目的页面做检查，恶意攻击者可以发送给用户一个伪装的链接，但是用户打开后，跳转至钓鱼网站页面，将会导致用户被钓鱼攻击，账号被盗，或账号相关财产被盗。
STC-8	水平权限攻击测试	高	Web 应用程序接收到用户请求，对用户数据进行 CRUD(增加、读取、更新和删除)操作时，没有判断数据的所属人，或数据所属人 userid 直接从用户提交的 request 参数（用户可控数据）中获取，导致恶意攻击者可以通过变换数据 ID 或所属人 userid，从而越权获取或修改其他人数据。
STC-9	垂直权限攻击测试	高	垂直权限攻击即低权限用户越权利用更高权限用户的功能实现权限提升攻击，是由于 web 应用程序没有做权限控制，或仅仅在菜单上做了权限控制，导致恶意用户只要猜测到其他管理页面的 URL，就可以访问或控制其他角色拥有的数据或页面，达到权限提升目的。

6.3 平台运维管理

6.3.1 安全保障方案

运营方应组织编制安全保障方案并报管理方审定。安全保障对象应包括粤省事移动政务服务平台、业务系统、政务云平台、政务网络等。

6.3.2 预警与预案

运营方和接入方应在省信息安全管理部门的指导下，加强网络安全监测预警技术能力建设。

运营方和接入方应按信息安全预案做好应急保障工作，定期组织演练，并向管理方报告信息安全事件情况。

6.3.3 突发事件处理

突发事件包含但不限于粤省事小程序和业务系统服务不可用、用户信息泄露、粤省事公众号推文引发舆情事件等。根据统一指挥、密切协同、快速反应、科学处置、预防为主、预防与应急相结合的原则，突发事件处理分工如下：

a) 管理方负责统一指挥和协调应急工作；

b) 接入方负责业务系统的突发事件预防、监测、报告和应急处置工作；

c) 运营方负责粤省事移动政务服务平台和政务云平台、政务网络的突发事件预防、监测、报告和应急处置工作。

接入方和运营方一旦发现突发事件，应立即通知管理方，不应迟报、漏报、瞒报、谎报。报告突发事件时，应列明事件发生时间、初步判定的影响范围和危害、已采取的应急处置措施和下一步工作建议。

参考文献

[1] C 0103 国家政务服务平台政务服务移动端建设要求
[2] 国办函〔2016〕108号 国务院办公厅关于印发“互联网+政务服务”技术体系建设指南的通知
[3] 广东省电子政务云平台管理暂行办法