ICS
L

CIIA

团 体 标 准

T/ CIIA xxx---xxxx

政务应用 APP
安全要求和检测方法

The Requirements and Detection Methods of Security for Government Application APP

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国信息协会 发布

目 录

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。

本文件由中国信息协会提出并归口。

本文件起草单位：国家信息中心、应急管理部通信信息中心、北京市电子产品质量检测中心、深圳海云安网络安全技术有限公司、新华三技术有限公司、江苏通付盾信息安全科技有限公司、蓝信移动（北京）科技有限公司、深信服科技股份有限公司、华为技术有限公司、博雅正链（北京）科技有限公司、河南芯盾网安科技发展有限公司。

本文件主要起草人：禄凯、任金强、王笑强、陈永刚、章恒、张羽、赵增振、李振平、黄玉钏、刘振峰、李桂杰、谢朝海、李刚、刘姝麟、马一云、汪德嘉、张昀球、裴利杰、韩炯、张航、张晗、周蓬、李文兴、李青山、王飞、罗东平、王靖。

政务应用 APP 安全要求和检测方法

1 范围

本文件规定了政务应用APP的安全技术要求、安全管理要求、个人信息保护要求和检测方法，为政务应用APP在设计阶段、开发阶段、发布阶段、运行维护阶段和废弃阶段等不同阶段的网络安全风险管控提供指导。

本文件适用于指导政府机构、运营单位、供应商、第三方服务单位等开展政务应用APP建设、开发、采购、管理、监管和测评工作。

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 25069-2010 信息安全技术 术语

GB/T 35282-2017 信息安全技术 电子政务移动办公系统安全技术规范

GB/T 34975-2017 移动智能终端应用软件安全技术要求和测试评价方法

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求

GB/T 35273-2020 信息安全技术 个人信息安全规范

C 0116-2018 国家政务服务平台网络安全保障要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

政务应用 APP

国家政务部门、企事业单位在政务活动中，利用现代信息技术、移动互联技术、办公自动化技术等进行办公、管理和为社会提供公共服务的移动智能终端应用程序。

3.2

政务公众号

国家政务部门、企事业单位在移动应用平台上申请的应用账号，通过公众号，国家政务部门、企事业单位可以在移动应用平台上实现和特定群体的文字、图片、语音、视频的全方位沟通、互动，进而进行办公、管理和为社会提供公共服务。

3.3

政务小程序

国家政务部门、企事业单位在统一的入口APP中提供的一种在移动终端无需下载安装，即可使用的应用。通过政务小程序可以进行办公、管理和为社会提供公共服务，用户在相关入口APP中通过扫一扫或者搜索即可打开并使用政务小程序。

3.4

政务应用

国家政务部门、企事业单位在政务活动中，利用现代信息技术、移动互联技术、办公自动化技术等进行办公、管理和为社会提供公共服务的应用软件系统。政务应用可以有不同的形式，如政务APP、政务公众号、政务小程序等。

3.5

政务敏感数据

政务敏感数据包括：

身份鉴别数据、密钥数据、电子证照数据、电子印章数据、访问控制数据、重要信息资源敏感标记数据、视频监控音像记录、电子门禁系统进出记录等数据。数据泄露、篡改、丢失后将对政务应用系统直接造成整体性危害。

姓名、身份证号、银行账号、联系方式、地址信息、偏好信息、健康信息等涉及自然人、法人的隐私信息。数据泄露后将对自然人、法人造成直接影响和利益损害。

办件信息、办结信息、督办信息、统计信息等涉及自然人、法人的业务信息。数据泄露、篡改、丢失后将对自然人、法人造成一定程度影响。

3.6

政务高风险业务

政务应用中，涉及修改政务敏感数据的功能，或者涉及操作现实或虚拟货币的业务，属于政务高风险业务，需要考虑增强级的安全防护机制。

3.7

基础级要求和增强级要求

基础级要求对应GB/T 22240-2020中规定的二级及以下应用。

增强级要求对应GB/T 22240-2020中规定的三级及以上应用。

4 缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Programming Interface）

FAQs：经常被提出的问题（Frequently Asked Questions）

HTTPS：超文本传输安全协议（Hyper Text Transfer Protocol over Secure Socket Layer）

SQL：结构化查询语言（Structured Query Language）

5 政务应用 APP 安全特性

5.1 政务应用 APP 安全技术模型

政务应用 APP 安全技术模型如图 1 所示，包括安全技术要求、安全管理要求、个人信息保护、检测

方法和安全特性。其中安全技术要求、安全管理要求、个人信息保护、检测方法是为保证政务应用 APP 安全特性所采取的具体技术或管理手段，而安全特性是政务应用 APP 的安全属性。政务应用 APP 安全特性具体包括完整性、保密性、可用性、不可否认性和可控性。政务应用 APP 会涉及大量国家、个人敏感信息，需要保证更高的安全特性，对安全技术也有更高的要求。

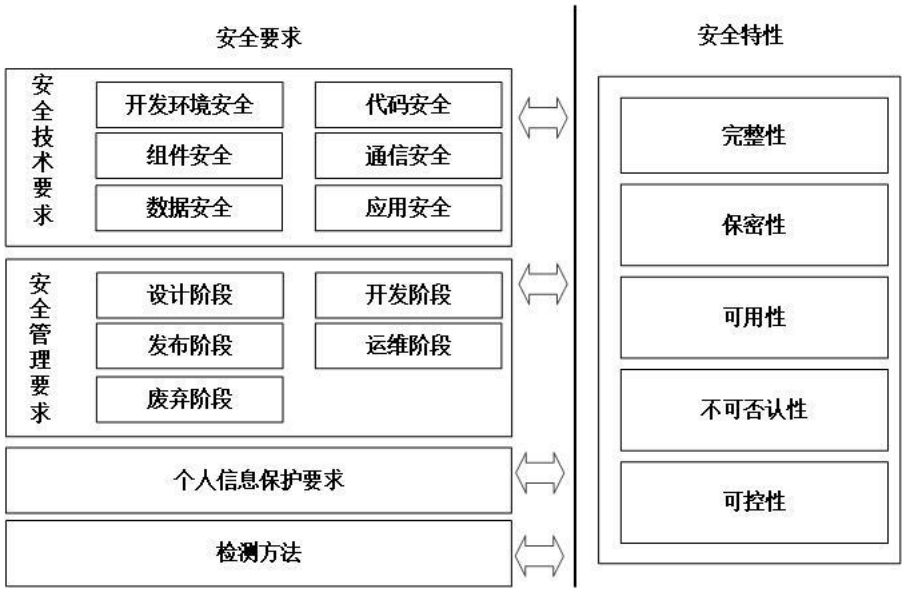

图 1 政务应用 APP 安全技术参考模型

5.2 完整性

指政务信息在传输、交换、存储和处理过程保持非修改、非破坏和非丢失的特性，即保持信息原样性，使信息能正确生成、存储、传输，这是最基本的安全特征。

政务应用 APP 集政务事务公开，社会新闻实时更新，在线生活缴费、缴税，个人、企业信息统计查询,紧急预警等与老百姓息息相关的功能于一体,涉及政府形象便民工程,所以需要加大安全力度建设，保证政务应用 APP 的完整性。

5.3 保密性

指政务信息按给定要求不泄漏给非授权的个人、实体或过程，或不提供其利用的特性，即杜绝有用信息泄漏给非授权个人或实体，强调有用信息只被授权对象使用的特征。

政务应用 APP 主要业务包括用户实名登记、开户信息备案、政务办公受理及收费、集客异步受理和资料归档等业务场景，涉及用户身份证、照片、个人及企业信息、开户时个人及企业信息的审核结果等敏感信息的处理，同时为用户提供账户缴费、查询、交易等多种服务，涉及到政务业务安全和数据存储安全，需要加强政务应用 APP 在开发、测试、发布和运营过程中的安全性，并增强数据保密性，防止发生信息泄露、篡改等安全事件。

5.4 可用性

指网络信息可被授权实体正确访问，并按要求能正常使用或在非正常情况下能恢复使用的特征，即在系统运行时能正确存取所需信息，当系统遭受攻击或破坏时，能迅速恢复并能投入使用。可用性是衡量网络信息系统面向用户的一种安全性能。

电子政务网络系统由核心网、承载网、业务网、传输网、服务网等组成，基于这些网络的业务和数

据处理正面临严重的安全威胁，需要搭建网络安全支撑平台及容灾备份系统，并限制授权用户及管理员访问。

5.5 不可否认性

指通信双方在信息交互过程中，确信参与者本身，以及参与者所提供的信息的真实同一性，即所有参与者都不可能否认或抵赖本人的真实身份，以及提供信息的原样性和完成的操作与承诺。

随着“互联网+政务”开启政务服务新时代的到来，使得政务应用 APP 涉及大量数据需要在网络中传输、共享，重要信息或私有化信息存在被拦截、窃取的可能，对传输数据的保密性带来了威胁，需要对证书加密，并增加证书校验功能，对协议结构进行二次封包，对数据进行加密处理。防止黑客通过使用第三方代理抓包工具动态抓取客户端与服务端传输的数据包，窃取传输的关键数据。

5.6 可控性

指对流通在网络系统中的信息传播及具体内容能够实现有效控制的特性，即网络系统中的任何信息要在一定传输范围和存放空间内可控。除了采用常规的传播站点和传播内容监控这种形式外，最典型的如密码的托管政策，当加密算法交由第三方管理时，必须严格按规定可控执行。

政务应用 APP 的广泛应用，涉及国家信息安全，需要结合多种先进的安全防护和监控手段做到风险可控，提升移动应用的安全防护能力，实现安全可控。

6 安全技术要求

6.1 开发环境安全

6.1.1 基础级

a) 应保证开发环境的可靠性，严格审核应用程序、第三方代码和库文件，以确定业务的需要，并验证功能的安全性；
b) 应保证开发环境的完整性和一致性，使用校验和或哈希值验证编译后的代码、库文件、可执行文件和配置文件；
c) 应保证开发环境的保密性，应具备对口令猜测的防范机制和监控手段；
d) 应严格控制开发环境的用户权限，分等级分层次对开发环境的用户权限进行最小化、规范化处理。

6.1.2 增强级

a) 开发环境的登录应具备双因子或多因子认证措施；
b) 开发环境应具备审计措施，记录开发者的登录和操作行为；
c) 开发环境应具备恶意代码防范能力；
d) 开发环境与生产环境之间应采取隔离及监控措施。

6.2 代码安全

6.2.1 基础级

a) 应使用死锁来防止多个同时发送的请求，或使用一个同步机制防止竞态条件；
b) 应在函数的开头部分明确初始化所有变量；
c) 应禁止在代码或代码注释中写入敏感信息；
d) 应以安全的方式访问数据库，严格定义数据库用户的角色和权限；

e） 应确保开发接口的安全性；
f） 应防范应用程序中不可信数据被解析为命令或查询语句等；
g） 应采用防逆向工程保护措施，防范攻击者对客户端应用软件的反编译分析；
h） 应采用签名校验机制，防止应用程序被二次打包。

6.2.2 增强级

无。

6.3 组件安全

6.3.1 基础级

a） 应配置安全权限，只允许授权用户导出组件；
b） 应遵循最小化组件暴露的原则；
c） 应对暴露组件进行代码检测，并通过自定义权限限制对它的调用；
d） 应具备防止组件遭受拒绝服务攻击的能力，防止异常出现；
e） 应具备恶意代码防范能力。

6.3.2 增强级

无。

6.4 通信安全

6.4.1 基础级

a） 在通信的建立过程中,客户端对服务器端的证书进行有效性验证，校验证书的域名、证书颁发机构等；
b） 客户端和服务器之间的通信使用加密信道,加密方式应满足国家密码管理部门要求；
c） 客户端向服务器发送密码的时候，应对密码进行加密传输。

6.4.2 增强级

在客户端预先存储服务器的证书公钥，在通信建立时，客户端获取服务器证书公钥，并和本地存储的公钥进行比较。

6.5 数据安全

6.5.1 数据输入安全

6.5.1.1 基础级

a） 应严格控制移动终端数据输入，进行必要的有效性检查，防止SQL注入、跨站脚本攻击、本地文件包含等攻击；
b） 应防止在登录过程中默认保存用户上次的账号及口令信息。

6.5.1.2 增强级

应采取有效防护措施，防止敏感数据在输入过程中被截获或篡改。

6.5.2 数据访问安全

6.5.2.1 基础级

a) 应限制对存有政务敏感信息的结构型数据的访问，保证敏感数据仅供授权用户或授权应用组件访问；
b) 应对客户端政务应用APP所在目录的文件权限进行设置，不允许其他组成员读写。

6.5.2.2 增强级

应使用安全机制保证API调用的安全。

6.5.3 数据存储安全

6.5.3.1 基础级

a) 内部存储中的政务敏感数据应加密存储；
b) 应避免在缓存文件和外部存储保存敏感数据；
c) 应避免在日志中记录敏感数据；
d) 卸载政务APP后，无相关残留文件。

6.5.3.2 增强级

a) 操作系统的备份文件中不应保存有敏感数据；
b) 内存中的敏感数据应设置最大保存时间，超过时间应进行删除。

6.5.4 数据输出安全

6.5.4.1 基础级

a) 应避免明文显示密码；
b) 系统运行时应默认禁止输出调试信息；
c) 如开启了调试功能，应避免调试日志暴露敏感数据；
d) 应对系统提示信息中用户的敏感数据进行加密保护；
e) 客户端页面回退应清除敏感数据；
f) 应避免在系统技术错误信息中出现敏感数据。

6.5.4.2 增强级

无。

6.6 应用安全

6.6.1 会话安全

6.6.1.1 基础级

a) 会话标识应保持唯一、随机、不可猜测机制；
b) 会话过程中应维持认证状态；
c) 退出登录或移动应用关闭后，应立即终止会话；
d) 对于非消息推送类应用，会话应设置超时时间，当空闲时间超过设定时间应自动终止会话；
e) 会话结束后，应及时清除会话信息；
f) 应对系统的最大并发会话连接数进行限制；
g) 当应用系统通信双方中的一方在指定时间内未作任何响应，另一方应自动结束会话；

h） 应设置访问令牌机制，访问令牌应动态随机生成。

6.6.1.2 增强级

a） 应支持限制单个用户同时登录的会话个数；
b） 应支持用户查看最近登录设备；
c） 应对涉及关键应用的操作提供会话保护机制。

6.6.2 认证安全

6.6.2.1 基础级

a） 使用账号口令进行登录时，应使用授权认证令牌的方法来取代口令，在传输时进行加密，后端服务器进行验证；
b） 应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施；
c） 更改用户口令时，应对用户的身份进行有效验证；
d） 手机短信验证码或动态口令应随机产生，长度不少于6位；
e） 手机短信验证码或动态口令应设定有效时间，超过有效时间应立即作废。

6.6.2.2 增强级

针对高风险业务，应采用两种或两种以上组合的鉴别技术对用户进行身份认证鉴别。

6.6.3 口令安全

6.6.3.1 基础级

a） 应避免明文显示口令；
b） 使用系统初始化口令首次登录时，应强制用户修改初始口令；
c） 应具有自动检验弱口令的能力；
d） 应及时加密口令；
e） 口令应避免保存在移动终端本地。

6.6.3.2 增强级

无。

6.6.4 访问安全

6.6.4.1 基础级

应支持设置超时退出策略。

6.6.4.2 增强级

a） 关键信息页面应防范被截屏、拍照泄密的风险，如采用屏幕水印技术；
b） 应支持管理员强制打开屏幕锁功能；
c） 应具备冻结用户功能，避免风险用户访问系统。

6.7 其他安全

6.7.1 公众号安全

6.7.1.1 基础级

a） 应进行敏感词自动检查，发布内容中存在敏感内容时进行提示；
b） 系统应对公众号发布过程及发布内容进行记录审计；
c） 公众号发布的内容应可管理、修改和撤销。

6.7.1.2 增强级

公众号发布流程应设置审核员，对内容进行人工审核。

6.7.2 应用接入安全

6.7.2.1 基础级

a） 系统应为对接应用提供应用账号及口令或验证码，调用时需对应用进行身份认证；
b） 系统应对应用进行审核，仅经过审核的应用允许上线；
c） 系统应对应用发布过程及发布内容进行记录审计；
d） 系统对于小程序应用，应提供签名校验机制；
e） 应对应用接口进行授权管理，确保应用仅获取用户同意提供的用户信息。

6.7.2.2 增强级

无。

7 安全管理要求

7.1 设计阶段

7.1.1 基础级

a）应对政务应用的安全需求进行分析，形成安全需求文档；
b）应采用威胁建模等方法形成政务应用安全威胁模型，分析可能遭受的各类攻击和潜在风险；
c）应对政务应用的架构设计进行分析，确保所有组成部分均被识别并且评估该组成部分的必要性。

7.1.2 增强级

a）应确保安全控制措施不仅仅在客户端存在，在服务端也有相应的安全控制措施；
b）应确保政务应用中出现的敏感信息都被识别；
c）应确保加密密钥遵循明确的策略进行管理；
d）应确保设计了强制更新的机制。

7.2 开发阶段

7.2.1 基础级

a） 应遵循安全需求和安全设计的要求，对所开发的政务应用APP实施相应的安全控制措施；
b） 应形成政务应用APP代码安全规范并确保开发人员遵循相应的规范进行代码开发；
c） 应对开发的源代码进行安全设计和安全编码审查；
d） 应采用代码分析工具对开发的源代码进行扫描分析；

e） 应对源代码版本进行控制，保证当前系统始终为最新的稳定版本；
f） 应确保对程序资源库的修改、更新、发布进行授权和批准；
g） 应严格控制对源代码的访问。

7.2.2 增强级

a） 应对政务行业内开发人员进行安全意识及安全技能培训；
b） 如政务应用的开发涉及外包，应制定外包开发流程制度，对外包人员进行安全培训和外包管理。

7.3 发布阶段

7.3.1 基础级

a） 政务应用发布前，应经过审批过程，并形成审批记录；
b） 政务应用发布前，应对检测到的高危险漏洞及时进行修复；
c） 政务应用发布前，应采取必要措施，使所开发的政务应用拥有防止调试和防止逆向工程等能力；
d） 政务应用发布前，应采取必要措施，对所开发的政务应用进行代码混淆和加固等处理；
e） 政务应用发布前，应采取必要措施，确认调试接口已关闭；
f） 政务应用的发布版本与测试版本禁止使用同一服务端的API；
g） 发布的政务应用中，内容禁止涉及违法违规信息；
h） 发布的政务应用中，禁止包含测试代码；
i） 发布的政务应用，禁止输出日志信息；
j） 政务应用在卸载时，应删除运行时产生的所有缓存文件、日志文件等；
k） 政务应用在卸载时，禁止篡改、覆盖删除系统文件和其他软件；
l） 政务应用在卸载后，应确保系统环境仍正常运行。

7.3.2 增强级

发布的政务应用，应保证可检测终端，确认是否运行在特权用户环境，进行告警或停止运行。

7.4 运维阶段

7.4.1 人员管理

7.4.1.1 基础级

a） 应根据各个运维部门和岗位的职责明确政务应用APP的安全管理授权审批事项、审批部门和批准人；
b） 应针对政务应用APP变更、重要操作、物理访问和系统接入等事项执行审批过程；
c） 应保证政务应用APP安全管理服务端设置专职管理员、操作员，且权限由审批部门或批准人批准。

7.4.1.2 增强级

无。

7.4.2 资产管理

7.4.2.1 基础级

a) 应编制并保存与保护对象相关的政务应用APP资产清单，包括资产责任部门、重要程度和使用人等内容；
b) 应根据资产的重要程度对政务应用APP进行标识管理，根据其价值选择相应的管理措施。

7.4.2.2 增强级

无。

7.4.3 漏洞和风险管理

7.4.3.1 基础级

a) 应采取必要的措施识别政务应用APP安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修复整改；
b) 如发现重大安全漏洞应重点修复，并及时更新，未更新重大漏洞的版本不允许使用。

7.4.3.2 增强级

无。

7.4.4 恶意代码防范管理

7.4.4.1 基础级

应对政务应用APP恶意代码防范要求做出规定,包括防恶意代码软件的授权使用、恶意代码库升级、恶意代码的定期查杀等。

7.4.4.2 增强级

应对截获的恶意代码进行及时分析处理。

7.4.5 访问控制

7.4.5.1 基础级

a) 政务应用APP应建立访问控制策略，并基于业务和访问的安全要求进行评审；
b) 信息访问限制,防止对政务应用APP进行未授权访问；
c) 安全登录，应通过安全登录对政务应用APP进行访问；
d) 应用源代码访问控制，应对源代码做防护，限制对源代码进行访问。

7.4.5.2 增强级

无。

7.4.6 监测管理

7.4.6.1 基础级

a) 应对上线后的政务应用APP进行持续性监测预警,实时通报恶意、违法、有风险的政务应用APP；
b) 版本监测，应实时监测已发布的版本情况，确保政务应用APP保持最新的发布版本；
c) 内容监测，若存在用户信息发布功能，应对发布内容进行监测。涉及违法违规信息内容的，视情采取警示、限制功能、暂停更新、关闭账号等处置措施，保存记录，并向有关主管部门报告；

d) 实名监测，应确保应用开发者可溯源，每个移动应用开发者信息应做好详细记录，并保证发布平台上的政务应用APP的实名认证；
e) 应建立安全应急响应制度，针对不同等级的安全事件应能够快速响应，对于政务应用APP中发现的高危漏洞，应能在24小时内进行升级修补。

7.4.6.2 增强级

a) 应定期进行全面的风险评估，当组织的业务流程、系统状况发生重大变更时，也应进行风险评估。评估内容包括对真实运行的信息系统、资产、威胁、脆弱性等各方面；
b) 攻击监测，应对上线后的政务应用APP进行攻击行为监测，应保证上线后的政务应用APP运行的安全状态；
c) 分发监测，应确保发布渠道可溯源，且在符合法律法规要求的安全渠道分发，每个移动应用应加上渠道标签；
d) 仿冒监测，应保证实时监测已发布的政务应用APP在内网下载地址或互联网发布渠道中的状态，如图标、包名、签名、MD5等，确保政务应用APP不被仿冒。

7.4.7 安全意识培训

7.4.7.1 基础级

a) 应对管理、开发及运维人员进行政务应用APP安全意识教育培训，并告知相关的安全责任和惩戒措施；
b) 应对政务应用APP设置专职管理员、操作员进行专项安全意识教育和岗位技能培训，并告知相关的安全责任和惩戒措施。

7.4.7.2 增强级

无。

7.5 废弃阶段

7.5.1 废弃处置

7.5.1.1 基础级

a) 确保废弃政务应用APP的资产及残留信息得到适当的处置，确保系统组件被合理的丢弃或更换；
b) 确定政务应用APP废弃后相关联的系统连接是否关闭，若被废弃的系统是某个系统的一部分，或与其他系统存在物理或逻辑的连接，都需要做关闭处理；
c) 如果在系统变更中废弃，除对废弃部分外，还应对变更的部分进行评估，以确定是否会增加风险或引入新的风险。

7.5.1.2 增强级

无。

7.5.2 废弃声明

7.5.2.1 基础级

政务应用APP废弃声明，将停止运营的通知以逐一送达或公告的形式通知。

7.5.2.2 增强级

无。

7.5.3 安全卸载

7.5.3.1 基础级

a) 政务应用APP在卸载时，应严格依据登记注册的卸载项，逐项删除清理，如涉及到资金交易等敏感信息，须删除运行时产生的所有缓存文件、日志文件等，同时不得篡改、覆盖、删除系统文件和其他软件，确保卸载后系统环境正常运行；
b) 政务应用APP在停止运营前，应明确告知用户，并停止使用用户个人信息，并对已保存的数据进行删除或匿名化处理。

7.5.3.2 增强级

无。

8 个人信息保护要求

8.1 安全收集

8.1.1 基础级

a) 收集个人信息前应提供让用户主动选择同意或不同意的选项，不同意应仅影响与所拒绝提供个人信息相关的业务功能；
b) 应制定隐私政策，并通过弹窗、文本链接、常见问题（FAQs）等形式告知用户；
c) 隐私策略应对应用运营者基本情况进行描述，包括：公司名称、注册地址、常用办公地点和相关负责人的联系方式等；
d) 隐私政策应以单独成文的形式发布，而不是作为用户协议、用户说明等文件中的一部分存在；
e) 隐私政策中应将收集个人信息的业务功能逐项列举，逐一说明每个业务功能收集哪些个人信息类型，避免使用“等、例如”字样；
f) 隐私政策应对个人敏感信息类型进行显著标识，如字体加粗、标星号、下划线、斜体、颜色等；
g) 隐私政策中至少提供以下一种投诉渠道：电子邮件、电话、传真、在线客服、在线表格；
h) 在用户安装、注册或首次开启政务应用时，应主动提醒用户阅读隐私政策。当政务应用打开系统权限时，应说明该权限收集个人信息的目的。收集个人敏感信息时，政务应用应通过弹窗提示等显著方式向用户明示收集、使用个人敏感信息的目的、方式、范围；
i) 应避免第三方SDK非法收集个人信息。

8.1.2 增强级

无。

8.2 安全保存

8.2.1 基础级

a) 隐私政策应对个人信息存放地域（国内、国外）、存储期限、超期处理方式进行明确说明；
b) 个人信息收集后，应立即进行去标识化处理，采取技术和管理方面的措施，将去标识化后的数据与可用于恢复识别的个人信息分开存储；

c） 传输和存储个人敏感信息时，应采用加密等安全措施；
d） 个人生物识别信息存储时，应采取技术措施处理后再进行存储，例如：仅存储个人生物识别信息的摘要；
e） 个人信息保存期限应为实现目的所必需的最短时间；
f） 停止运营时，应及时停止继续收集个人信息的活动，应将停止运营的通知逐一送达或公告的形式通知用户，应对所持有的个人信息进行删除或匿名化处理。

8.2.2 增强级

无。

8.3 安全使用

8.3.1 基础级

a） 应遵循最小化授权原则对个人信息采取访问控制措施；
b） 对于需要通过界面展示个人信息的，应对其采取去标识化处理等措施；
c） 将个人信息用于用户画像、个性化展示等用途时，隐私政策中应说明其应用场景和可能对用户产生的影响；
d） 应提供查询、更正、删除个人信息的途径；
e） 应提供注销账号的途径（在线功能界面、客户电话等），并在用户注销账号后，及时删除其个人信息或进行匿名化处理；
f） 如果存在个人信息对外共享、转让、公开披露等情况，应征得用户同意，隐私政策中应明确以下内容：
   1）对外共享、转让、公开披露个人信息的目的；
   2）涉及的个人信息类型；
   3）接收方类型或身份；
g） 如果存在个人信息出境情况，隐私政策中应将出境个人信息类型逐项列出并显著标识（如字体加粗、标星号、下划线、斜体、颜色等）。

8.3.2 增强级

无。

9 安全技术要求检测方法

9.1 开发环境安全检测方法

9.1.1 测试对象

开发环境下的操作系统、应用程序、第三方代码、库文件、配置文件。

9.1.2 测试方法

9.1.2.1 基础级

a） 检查审核操作系统、应用程序、第三方代码和库文件，是否为最小部署原则，是否具备核验可靠性措施；
b） 检查开发环境对编译后的代码、库文件、可执行文件和配置文件是否具备校验机制；

c） 检查操作系统、应用程序的访问控制，判断是否具备对口令猜测的防范机制和监控手段；
d） 检查开发环境的用户或用户组权限，判断是否具备权限最小化、规范化处理。

9.1.2.2 增强级

a） 检查和验证开发环境是否具备双因子或多因子身份认证方式；
b） 检查开发环境是否具备和开启了安全审计功能；
c） 检查开发环境是否具备恶意代码防范功能；
d） 检查开发环境与生产环境之间是否采取隔离及监控措施。

9.1.3 预期结果

9.1.3.1 基础级

a） 操作系统、应用程序、第三方代码和库文件均为最小化部署，具备授权管理和或安全核验机制；
b） 开发环境对编译后的代码、库文件、可执行文件和配置文件具备校验机制；
c） 操作系统、应用程序具备访问控制功能；
d） 开发环境的用户或用户组权限，进行了权限最小化、规范化处理。

9.1.3.2 增强级

a） 开发环境具备双因子或多因子身份认证方式；
b） 开发环境具备和开启了安全审计功能；
c） 开发环境具备恶意代码防范功能；
d） 开发环境与生产环境之间具备隔离及监控措施。

9.1.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

9.2 代码安全检测方法

9.2.1 测试对象

源代码、编译后的代码。

9.2.2 测试方法

9.2.2.1 基础级

a） 采用人工代码审查方法或借助代码分析工具，判断代码是否采用了死锁来防止多个同时发送的请求，或使用一个同步机制防止竞态条件；
b） 检查是否在函数的开头部分明确初始化了所有变量；
c） 检查在代码或代码注释中是否写入了敏感信息，检查是否存在关键词如“AES_key”、“DES_key”、“username”、“password”、IP地址等，并进一步分析确认是否是账号密码、数据密码、内网IP地址等敏感信息；
d） 检查客户端代码是否以安全的方式访问数据库，严格定义了数据库用户的角色和权限；
e） 检查客户端代码是否以安全的方式调用其他开发接口；
f） 检查代码中是否有防范应用程序中不可信数据被解析为命令或查询语句等的措施；
g） 检查代码中是否采用了防逆向工程的保护措施，防范攻击者对客户端应用软件的反编译分析；

h） 检查代码是否采用了签名校验机制，防止应用程序被二次打包。

9.2.2.2 增强级

无。

9.2.3 预期结果

9.2.3.1 基础级

a） 采用了死锁来防止多个同时发送的请求，或使用一个同步机制防止竞态条件；
b） 在函数的开头部分明确初始化了所有变量；
c） 未检索到敏感信息；
d） 代码以安全的方式访问数据库，严格定义了数据库用户的角色和权限；
e） 客户端代码以安全的方式调用其他开发接口；
f） 有防范应用程序中不可信数据被解析为命令或查询语句等的措施；
g） 采用了防逆向工程的保护措施，防范攻击者对客户端应用软件的反编译分析；
h） 采用了签名校验机制，防止应用程序被二次打包。

9.2.3.2 增强级

无。

9.2.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

9.3 组件安全检测方法

9.3.1 测试对象

政务应用APP组件。

9.3.2 测试方法

9.3.2.1 基础级

a） 检查是否只有需要导出的组件才导出；
b） 检查需要导出的组件，是否使用自定义权限限制调用；
c） 检查自定义权限等级是否为signature和signatureOrSystem；
d） 使遍历APP所有导出组件，观察界面错误提示，并监控崩溃日志；
e） 检测组件是否具备恶意代码防范能力。

9.3.2.2 增强级

无。

9.3.3 预期结果

9.3.3.1 基础级

a） 只有需要导出的组件才设置为导出；

b) 导出的组件使用自定义权限限制调用；
c) 自定义权限等级为signature和signatureOrSystem；
d) 未发现程序崩溃和错误提示；
e) 具备恶意代码防范能力。

9.3.3.2 增强级

无。

9.3.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

9.4 通信安全检测方法

9.4.1 测试对象

通信协议、传输数据。

9.4.2 测试方法

9.4.2.1 基础级

a) 使用工具生成任意证书，进行中间人攻击；而后再生成指定域名的证书，进行中间人攻击；
b) 抓取数据包，检查APP是否以明文形式传输用户数据；
c) 检查APP客户端是否在发送密码前对其进行了加密,加密方式是否满足国家密码管理部门要求。

9.4.2.2 增强级

使用工具对APP实施HTTPS中间人攻击。

9.4.3 预期结果

9.4.3.1 基础级

a) 使用任意伪造证书进行中间人攻击，无法通过证书验证；使用指定域名的伪造证书，可以和客户端建立连接，并读取报文；
b) 可以看到客户端和服务器之间以密文形式传输数据；
c) 客户端向服务器发送的密码已做加密处理，加密方式满足国家密码管理部门要求。

9.4.3.2 增强级

无法和客户端建立连接，攻击失败。

9.4.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

9.5 数据安全检测方法

9.5.1 数据输入安全检测方法

9.5.1.1 测试对象

输入数据。

9.5.1.2 测试方法

9.5.1.2.1 基础级

a) 用户输入数据包含各种特殊字符（如单引号、双引号、尖括号、空格等），超长字符，数字型的边界值；
b) 用户将APP切换到后台，再次切换回前台；用户退出APP后再次打开。

9.5.1.2.2 增强级

检查政务应用APP是否采用安全键盘，是否具备防界面劫持和防截屏录屏功能。

9.5.1.3 预期结果

9.5.1.3.1 基础级

a) 系统提示，输入错误；
b) 会进入用户登录界面，不会自动登录。

9.5.1.3.2 增强级

不能进行截屏录屏操作,或者截取的为空图像或文件;采用了安全键盘功能,具备防界面劫持功能。

9.5.1.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

9.5.2 数据访问安全检测方法

9.5.2.1 测试对象

应用数据权限。

9.5.2.2 测试方法

9.5.2.2.1 基础级

a) 检查是否有安全措施限制敏感数据仅供授权用户或授权应用组件访问；
b) 查看APP所在目录的文件系统和文件权限。

9.5.2.2.2 增强级

检查是否使用安全机制进行验证，如：令牌+签名认证。

9.5.2.3 预期结果

9.5.2.3.1 基础级

a) 具备安全措施限制敏感数据仅供授权用户或授权应用组件访问；
b) 该APP所在目录文件其他组用户不可读写。

9.5.2.3.2 增强级

具备安全机制进行验证，如：令牌+签名认证。

9.5.2.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

9.5.3 数据存储安全检测方法

9.5.3.1 测试对象

存储数据、开发人员。

9.5.3.2 测试方法

9.5.3.2.1 基础级

a) 检查内部存储文件中的敏感数据是否进行加密；
b) 检查缓存文件以及外部存储是否保存有敏感数据；
c) 查看日志，是否有敏感信息；
d) 手机上卸载APP后，查找相关残留文件。

9.5.3.2.2 增强级

a) 检查操作系统的备份文件中是否保存有敏感数据；
b) 访谈开发人员对于内存中敏感数据是否设置了保存时间。

9.5.3.3 预期结果

9.5.3.3.1 基础级

a) 内部存储文件中没有明文存储的敏感数据；
b) 缓存文件以及外部存储中没有保存敏感数据；
c) 日志中没有敏感数据；
d) 无相关残留文件。

9.5.3.3.2 增强级

a) 操作系统的备份文件中没有保存敏感数据；
b) 内存中敏感数据设置了最大保存时间。

9.5.3.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

9.5.4 数据输出安全检测方法

9.5.4.1 测试对象

输出数据。

9.5.4.2 测试方法

9.5.4.2.1 基础级

a) 在用户界面，输入密码；
b) 检查默认情况下，是否开启调试功能；
c) 开启调试功能，查看调试日志；
d) 查看系统提示信息；
e) 客户端页面回退；
f) 查看系统错误信息。

9.5.4.2.2 增强级

无。

9.5.4.3 预期结果

9.5.4.3.1 基础级

a) 用户界面不会明文显示密码；
b) 默认情况下，调试功能禁用；
c) 调试信息中不含有敏感数据；
d) 提示信息中涉及的用户敏感信息进行了加密等保护措施；
e) 客户端页面回退，敏感信息均已被清除；
f) 系统错误信息中不含有敏感数据。

9.5.4.3.2 增强级

无。

9.5.4.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

9.6 应用安全检测方法

9.6.1 会话安全检测方法

9.6.1.1 测试对象

传输数据、政务应用APP。

9.6.1.2 测试方法

9.6.1.2.1 基础级

a) 使用不同的用户登录客户端进行正常操作，进行抓包分析，并分析操作日志；
b) 在一定时间内无操作，检查是否会话超时，要求重新登录；
c) 根据会话数量限制规则，使用多客户端并发连接；
d) 登出客户端后，再进入客户端查看登出用户是否还能使用；
e) 利用工具抓包回放，利用返回信息判断是否能够重复调用。

9.6.1.2.2 增强级

a) 根据单个用户同时登录会话个数限制，使用同一个用户多次登录；
b) 查看用户最近登录设备；
c) 是否对涉及关键应用的操作提供会话保护机制。

9.6.1.3 预期结果

9.6.1.3.1 基础级

a) 抓包内容被加密，不同用户的会话令牌不一样，同一用户令牌唯一，而且每次登录产生的令牌不一样；
b) 非消息推送类应用，一段时间不操作会话过期重新登录；
c) 超过连接上限的会话无法连接；
d) 登出客户端后用户信息清除；
e) 利用工具抓包后重放失败。

9.6.1.3.2 增强级

a) 用户超出同时登录会话个数限制后，不能再次登录；
b) 用户可以查看最近登录设备列表；
c) 涉及关键应用操作时，采用多种方式进行会话保护。

9.6.1.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

9.6.2 认证安全检测方法

9.6.2.1 测试对象

政务应用APP。

9.6.2.2 测试方法

9.6.2.2.1 基础级

a) 使用账号口令进行登录；
b) 尝试多次输入密码错误，验证配置登录失败处理功能是否有效；
c) 修改用户口令；
d) 获取手机短信验证码后，超过一定时间后尝试验证。

9.6.2.2.2 增强级

针对高风险业务进行访问操作。

9.6.2.3 预期结果

9.6.2.3.1 基础级

a) 正常登录，无法从抓包中获取令牌信息；
b) 多次输入密码错误，能够触发登录失败处理功能；

c） 修改口令前需要先输入以前的口令；
d） 短信验证码大于等于6位，而且一定时间后验证码失效。

9.6.2.3.2 增强级

高风险应用使用两种或两种以上组合的鉴别技术对用户进行身份认证鉴别。

9.6.2.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

9.6.3 口令安全检测方法

9.6.3.1 测试对象

政务应用APP口令。

9.6.3.2 测试方法

9.6.3.2.1 基础级

a） 新建账户登录；
b） 使用系统初始化口令首次登录；
c） 使用弱口令修改设置用户名、口令；
d） 客户端输入用户名和口令登录，利用工具抓包；
e） 进行交易操作，验证是否需要重新输入支付口令。

9.6.3.2.2 增强级

无。

9.6.3.3 预期结果

9.6.3.3.1 基础级

a） 不使用明文显示口令；
b） 使用系统初始化口令首次登录，要求强制修改口令；
c） 弱口令提示，无法修改口令；
d） 无法从抓包中获取明文口令；
e） 需要重新输入支付口令。

9.6.3.3.2 增强级

无。

9.6.3.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

9.6.4 访问安全检测方法

9.6.4.1 测试对象

政务应用APP。

9.6.4.2 测试方法

9.6.4.2.1 基础级

检查是否可设置超时退出策略。

9.6.4.2.2 增强级

a) 确认关键信息页面是否有被截屏、拍照泄密的风险，有否相关防范措施；
b) 管理员是否可强制打开用户的屏幕锁；
c) 管理员冻结某个用户，尝试使用被冻结的用户登录访问系统。

9.6.4.3 预期结果

9.6.4.3.1 基础级

应用可以设置超时退出策略，设置后超出设定时间段不使用该应用，再次使用时需要重新认证登录。

9.6.4.3.2 增强级

a) APP运行时，界面不存在被截屏、拍照泄密的风险，或截屏画面存在水印；
b) 管理员可强制打开用户的屏幕锁功能，打开后所有用户需要设置屏幕锁密码；
c) 被冻结的用户无法登录访问系统。

9.6.4.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

9.7 其他安全检测方法

9.7.1 公众号安全检测方法

9.7.1.1 测试对象

政务公众号、管理人员。

9.7.1.2 测试方法

9.7.1.2.1 基础级

a) 确认系统敏感词设置，在公众号中发布含敏感词的内容；
b) 查看发布内容审计记录；
c) 修改、撤销发布内容。

9.7.1.2.2 增强级

设置审核员，对发布内容进行人工审核。

9.7.1.3 预期结果

9.7.1.3.1 基础级

a) 发布内容中存在敏感内容时会进行提示，并且无法发送成功；
b) 可以查看到发布内容审计记录；
c) 可以修改、撤销发布内容。

9.7.1.3.2 增强级

设置审核员后，公众号发布的内容需要审核员审核通过后才能被普通用户看到。

9.7.1.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

9.7.2 应用接入安全检测方法

9.7.2.1 测试对象

政务应用APP、小程序、其他接入应用。

9.7.2.2 测试方法

9.7.2.2.1 基础级

a) 检查应用对接过程及接口规范，确认是否可为对接应用提供应用账号及密钥，调用时是否需对应用进行身份认证；
b) 检查应用审核机制；
c) 查看应用发布过程审计记录；
d) 检查小程序应用下载运行过程，确认是否有签名校验机制；
e) 检查对接应用运行过程，确认是否有用户授权过程，应用是否能获取用户同意范围外的信息。

9.7.2.2.2 增强级

无。

9.7.2.3 预期结果

9.7.2.3.1 基础级

a) 可为对接应用提供应用账号及密钥，调用时需对应用进行身份认证；
b) 有应用审核机制，仅经过审核的应用允许上线；
c) 可查看应用发布过程审核记录；
d) 小程序应用下载运行时，有签名校验机制；
e) 对接应用运行时，有用户授权过程，应用仅能获取用户同意范围内的信息。

9.7.2.3.2 增强级

无。

9.7.2.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

10 安全管理要求检测方法

10.1 设计阶段安全管理检测方法

10.1.1 测试对象

技术文档、管理文档、记录文档。

10.1.2 测试方法

10.1.2.1 基础级

a) 检查是否编写了安全需求和安全设计相关文档；
b) 检查安全威胁模型及相关文档，查看是否有列明可能遭受的各类攻击和潜在风险；
c) 检查架构设计评审记录，查看是否对所有组成部分均作出识别并且评估了该组成部分的必要性。

10.1.2.2 增强级

a) 检查架构设计及相关文档，查看相关安全控制措施是否仅在客户端存在；
b) 检查架构设计及相关文档，查看在政务应用APP中出现的敏感信息是否均被识别；
c) 检查架构设计及相关文档，查看加密密钥是否遵循明确的策略进行管理；
d) 检查架构设计及相关文档，是否设计了强制更新的机制。

10.1.3 预期结果

10.1.3.1 基础级

a) 有相应的安全需求文档和安全设计文档；
b) 有分析并列明可能遭受的各类攻击和潜在风险；
c) 有架构设计评审记录，并且对所有组成部分均作出识别并且评估了该组成部分的必要性。

10.1.3.2 增强级

a) 架构设计等相关材料表明，安全控制措施不仅仅在客户端存在，在后端也有相应的安全控制措施；
b) 架构设计等相关材料表明，出现的敏感信息均被识别；
c) 架构设计等相关材料表明，加密密钥遵循了明确的策略进行管理；
d) 架构设计等相关材料表明，设计了强制更新的机制。

10.1.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

10.2 开发阶段安全管理检测方法

10.2.1 测试对象

开发人员、管理人员、技术文档、管理文档。

10.2.2 测试方法

10.2.2.1 基础级

a) 访谈和检查研发过程文档，判断开发人员是否遵循了安全需求和安全设计的要求，对所开发的政务应用实施了相应的安全控制措施；
b) 通过访谈或检查研发过程文档，判断是否形成了政务应用代码安全规范，且开发人员遵循了相应的规范进行代码开发；
c) 通过访谈或检查研发过程文档，判断是否对开发的源代码进行了安全设计和安全编码审查；
d) 通过访谈或检查研发过程文档，判断是否采用了代码分析工具对开发的源代码进行扫描分析；
e) 通过访谈或检查研发过程文档，判断是否对源代码版本进行了控制；
f) 通过访谈或检查研发过程文档，判断是否有规范的流程指导程序资源库的修改、更新、发布进行授权和批准；
g) 通过访谈或检查研发过程文档，判断是否对源代码的访问权限进行了严格的控制。

10.2.2.2 增强级

a) 通过访谈或检查培训记录等文档，判断是否对政务行业内开发人员进行了安全意识及安全技能培训；
b) 通过访谈或检查研发过程文档，判断政务应用的开发是否涉及外包，如涉及外包，是否制定了外包开发流程制度，是否对外包人员进行了安全培训和外包管理。

10.2.3 预期结果

10.2.3.1 基础级

a) 通过访谈结果和检查研发过程文档表明，开发人员遵循了安全需求和安全设计的要求，对所开发的政务应用实施了相应的安全控制措施；
b) 形成了政务应用代码安全规范，且开发人员遵循了相应的规范进行代码开发；
c) 对开发的源代码进行了安全设计和安全编码审查；
d) 采用了代码分析工具对开发的源代码进行扫描分析；
e) 对源代码进行了版本控制管理；
f) 遵循规范的流程，对程序资源库的修改、更新、发布进行授权和批准；
g) 对源代码的访问权限进行了严格的控制。

10.2.3.2 增强级

a) 对政务行业内开发人员进行了安全意识及安全技能培训；
b) 不涉及外包，或制定了外包开发流程制度且对外包人员进行了相应的培训和管控。

10.2.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

10.3 发布阶段安全管理检测方法

10.3.1 测试对象

政务应用、记录文档、管理人员、管理文档、技术文档。

10.3.2 测试方法

10.3.2.1 基础级

a) 检查政务应用发布前，是否经过审批过程，有相应的审批记录及文档；
b) 访谈和检查技术和管理文档，判断是否对检测到的高危险漏洞及时进行修复；
c) 检查技术文档和代码，判断是否内建了防止调试和防止逆向工程等能力；
d) 检查技术文档和代码，判断是否进行了代码混淆和加固等处理；
e) 检查技术文档和代码，判断调试接口是否已关闭；
f) 检查技术文档和代码，判断政务应用的发布版本与测试版本是否使用同一服务端的API；
g) 访谈和检查发布的政务应用中，内容是否包括违法违规信息；
h) 检查技术文档和代码，判断发布的政务应用中，是否包含测试代码；
i) 检查技术文档和代码，判断发布的政务应用，是否输出日志信息；
j) 访谈和检查政务应用在卸载时，是否删除运行时产生的所有缓存文件、日志文件等；
k) 访谈和检查政务应用在卸载时，是否篡改、覆盖删除系统文件和其他软件；
l) 访谈和检查政务应用在卸载后，系统环境是否仍正常运行。

10.3.2.2 增强级

检查政务应用，是否能够检测其在终端的运行环境，能够确认其是否运行在特权用户环境，并进行告警或停止运行。

10.3.3 预期结果

10.3.3.1 基础级

a) 政务应用发布前，已经过审批过程，并形成审批记录；
b) 政务应用发布前，已经对检测到的高危险漏洞及时进行修复；
c) 政务应用发布前,已采取必要措施,使所开发的政务应用拥有防止调试和防止逆向工程等能力；
d) 政务应用发布前，已采取必要措施，对所开发的政务应用进行代码混淆和加固等处理；
e) 政务应用发布前，已采取必要措施，确认调试接口已关闭；
f) 政务应用的发布版本与测试版本未使用同一服务端的API；
g) 发布的政务应用中，内容未包括违法违规信息；
h) 发布的政务应用中，未包含测试代码；
i) 发布的政务应用，未输出日志信息；
j) 政务应用在卸载时，已经删除运行时产生的所有缓存文件、日志文件等；
k) 政务应用在卸载时，未篡改、覆盖删除系统文件和其他软件；
l) 政务应用在卸载后，可确保系统环境仍正常运行。

10.3.3.2 增强级

发布的政务应用可检测其在终端的运行环境，如检测到运行在特权用户环境，应进行告警或停止运行。

10.3.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

10.4 运维阶段安全管理检测方法

10.4.1 人员管理检查

10.4.1.1 测试对象

管理人员、技术人员、管理文档、记录文档。

10.4.1.2 测试方法

10.4.1.2.1 基础级

a) 访谈检查各运维部门是否有安全管理授权审批事项、部门、批准人等流程；
b) 访谈检查政务应用APP变更、重要操作、物理访问和系统接入等事项执行中是否有审批过程；
c) 访谈检查政务应用APP安全管理服务端是否设置了专职管理员、操作员，权限由审批部门或批准人批准。

10.4.1.2.2 增强级

无。

10.4.1.3 预期结果

10.4.1.3.1 基础级

a) 运维部门具有安全管理授权审批事项、部门、批准人等流程和或文档；
b) 政务应用APP变更、重要操作、物理访问和系统接入等事项执行中具有审批过程和或文档；
c) 政务应用APP安全管理服务端已设置专职管理员、操作员，具有审批部门或批准人批准的流程和或文档。

10.4.1.3.2 增强级

无。

10.4.1.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

10.4.2 资产管理检查

10.4.2.1 测试对象

资产清单、记录文档。

10.4.2.2 测试方法

10.4.2.2.1 基础级

a) 检查是否具有政务应用APP资产清单；
b) 检查是具有政务应用APP标识。

10.4.2.2.2 增强级

无。

10.4.2.3 预期结果

10.4.2.3.1 基础级

a) 政务应用APP具有资产清单；
b) 政务应用APP具有标识信息。

10.4.2.3.2 增强级

无。

10.4.2.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

10.4.3 漏洞和风险管理检查

10.4.3.1 测试对象

技术人员、记录文档。

10.4.3.2 测试方法

10.4.3.2.1 基础级

a) 访谈政务应用APP是否具有发现安全漏洞和隐患的能力；
b) 检查漏洞修复记录、更新记录，访谈包含重大漏洞的是否不允许使用。

10.4.3.2.2 增强级

无。

10.4.3.3 预期结果

10.4.3.3.1 基础级

a) 具有对政务应用APP及时发现安全漏洞和隐患的能力；
b) 具有漏洞修复记录、更新记录，包含重大漏洞的不允许使用。

10.4.3.3.2 增强级

无。

10.4.3.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

10.4.4 恶意代码防范管理检查

10.4.4.1 测试对象

技术人员、管理文档。

10.4.4.2 测试方法

10.4.4.2.1 基础级

检查是否具有政务应用APP恶意代码防范要求做出规定。

10.4.4.2.2 增强级

访谈是否对截获的恶意代码进行分析处理。

10.4.4.3 预期结果

10.4.4.3.1 基础级

具有恶意代码防范要求的相关规定文档。

10.4.4.3.2 增强级

已对截获的恶意代码进行分析处理。

10.4.4.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

10.4.5 访问控制管理检查

10.4.5.1 测试对象

管理人员、技术人员。

10.4.5.2 测试方法

10.4.5.2.1 基础级

a) 访谈政务应用APP是否建立访问控制策略，是否基于业务和访问的安全要求进行了评审；
b) 访谈是否设置了信息访问限制；
c) 访谈是否具有安全登录功能；
d) 访谈是否具有应用源代码访问控制。

10.4.5.2.2 增强级

无。

10.4.5.3 预期结果

10.4.5.3.1 基础级

a) 建立了访问控制策略，并基于业务和访问的安全要求进行了评审；
b) 设置了信息访问限制；
c) 具有安全登录功能；
d) 具有应用源代码访问控制功能。

10.4.5.3.2 增强级

无。

10.4.5.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

10.4.6 监测管理检查

10.4.6.1 测试对象

管理平台、管理文档、技术文档、记录文档。

10.4.6.2 测试方法

10.4.6.2.1 基础级

a) 检查是否具有对上线后的政务应用APP进行持续性监测预警的功能或平台；
b) 检查是否具有版本监测功能；
c) 检查是否具有内容监测功能；
d) 检查是否具有实名监测功能，是否对移动应用开发者信息做详细记录；
e) 检查是否具有安全应急响应制度。

10.4.6.2.2 增强级

a) 检查是否具有全面的覆盖要求项的风险评估的记录；
b) 检查是否具有攻击监测功能；
c) 检查是否具有分发监测功能；
d) 检查是否具有仿冒监测功能。

10.4.6.3 预期结果

10.4.6.3.1 基础级

a) 具有对上线后的政务应用APP进行持续性监测预警的功能或平台；
b) 具有内容监测功能；
c) 具有版本监测功能；
d) 具有实名监测功能，是否具有移动应用开发者信息应做好详细记录；
e) 具有安全测试机构相关记录；
f) 具有安全应急响应制度。

10.4.6.3.2 增强级

a) 具有全面的覆盖要求项的风险评估的记录。
b) 具有攻击监测功能；
c) 具有分发监测功能；
d) 具有仿冒监测功能。

10.4.6.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

10.4.7 安全意识培训管理检查

10.4.7.1 测试对象

管理人员、开发人员、运维人员。

10.4.7.2 测试方法

10.4.7.2.1 基础级

a) 访谈管理、开发及运维人员是否进行了政务应用APP安全意识教育和岗位技能培训，是否知晓相关安全责任和惩戒措施；
b) 访谈政务应用APP的专职管理员、操作员是否进行了专项安全意识教育和岗位技能培训，是否知晓相关安全责任和惩戒措施。

10.4.7.2.2 增强级

无。

10.4.7.3 预期结果

10.4.7.3.1 基础级

a) 管理、开发及运维人员已进行了政务应用APP安全意识教育和岗位技能培训，并知晓相关安全责任和惩戒措施；
b) 政务应用APP已设置的专职管理员、操作员已进行了专项安全意识教育和岗位技能培训，并知晓相关安全责任和惩戒措施。

10.4.7.3.2 增强级

无。

10.4.7.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

10.5 废弃阶段安全管理检测方法

10.5.1 废弃处置管理检查

10.5.1.1 测试对象

管理人员、技术人员。

10.5.1.2 测试方法

10.5.1.2.1 基础级

a) 访谈废弃的政务应用APP的资产及残留信息是否妥当处理；
b) 访谈政务应用APP废弃后相关联的系统连接是否关闭；

c） 访谈移动应用系统相关硬件和软件等资产及残留信息是否得到了适当的处置；
d） 访谈当被废弃的APP系统是某个系统的一部分，或与其他系统存在物理或逻辑上的连接，与其他系统的连接是否被关闭；
e） 访谈在系统变更中废弃，除对废弃部分外，是否对变更的部分进行评估。

10.5.1.2.2 增强级

无。

10.5.1.3 预期结果

10.5.1.3.1 基础级

a） 已废弃的政务应用APP等资产及残留信息已妥当处理；
b） 政务应用APP废弃后相关联的系统连接已关闭；
c） 移动应用系统相关硬件和软件等资产及残留信息得到了适当的处置；
d） 当被废弃的APP系统是某个系统的一部分，或与其他系统存在物理或逻辑上的连接，与其他系统的连接已被关闭；
e） 在系统变更中废弃，除对废弃部分外，对变更的部分进行了评估。

10.5.1.3.2 增强级

无。

10.5.1.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

10.5.2 废弃声明管理检查

10.5.2.1 测试对象

管理文档、记录文档。

10.5.2.2 测试方法

10.5.2.2.1 基础级

检查是否具有政务应用APP废弃声明。

10.5.2.2.2 增强级

无。

10.5.2.3 预期结果

10.5.2.3.1 基础级

具有政务应用APP废弃声明。

10.5.2.3.2 增强级

无。

10.5.2.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

10.5.3 安全卸载管理检查

10.5.3.1 测试对象

技术文档、记录文档、管理人员。

10.5.3.2 测试方法

10.5.3.2.1 基础级

a) 检查政务应用APP在卸载时，是否做了删除清理敏感信息等操作；
b) 访谈政务应用APP在停止运营前，是否明确告知用户，并停止使用用户个人信息，对已保存的数据进行删除或匿名化处理。

10.5.3.2.2 增强级

无。

10.5.3.3 预期结果

10.5.3.3.1 基础级

a) 政务应用APP在卸载时，已删除了敏感数据；
b) 政务应用APP在停止运营前，已明确告知用户，并停止使用用户个人信息，对已保存的数据进行删除或匿名化处理。

10.5.3.3.2 增强级

无。

10.5.3.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

11 个人信息保护要求检测方法

11.1 安全收集检测方法

11.1.1 测试对象

政务应用、隐私政策文件。

11.1.2 测试方法

11.1.2.1 基础级

a) 启动运行政务应用，检查启动、登录、注册等会话界面，检查收集个人信息前是否提供了让用户主动选择同意或不同意的选项，如果选择不同意，检查是否仅影响与所拒绝提供个人信息相关的业务功能；
b) 借助工具或手动检查政务应用功能是否提供弹窗、文本链接、常见问题（FAQs）等形式的隐私政策；
c) 检查隐私政策中的各项描述是否符合个人信息保护的安全收集要求，是否对应用运营者基本情况进行描述，包括：公司名称、注册地址、常用办公地点和相关负责人的联系方式等；
d) 检查隐私政策是否以单独成文的形式发布，而不是作为用户协议、用户说明等文件中的一部分存在；
e) 检查隐私政策中是否将收集个人信息的业务功能逐项列举，并逐一说明每个业务功能收集哪些个人信息类型；
f) 检查隐私政策中是否对个人敏感信息类型进行了显著标识，如字体加粗、标星号、下划线、斜体、颜色等；
g) 检查隐私政策中是否至少提供了以下一种投诉渠道：电子邮件、电话、传真、在线客服、在线表格；
h) 检查在用户安装、注册或首次开启政务应用时，是否主动提醒用户阅读隐私政策。当政务应用打开系统权限时，检查政务应用是否提示用户并说明该权限收集个人信息的目的。收集个人敏感信息时，检查政务应用是否通过弹窗提示等显著方式向用户明示收集、使用个人敏感信息的目的、方式、范围；
i) 检查政务应用是否通过第三方SDK非法收集个人信息。

11.1.2.2 增强级

无。

11.1.3 预期结果

11.1.3.1 基础级

a) 政务应用在收集个人信息前提供了让用户主动选择同意或不同意的选项，如果选择不同意，仅影响与所拒绝提供个人信息相关的业务功能；
b) 提供了弹窗、文本链接、常见问题（FAQs）等形式的隐私政策；
c) 隐私政策中的各项描述符合个人信息保护的安全收集要求，对应用运营者基本情况进行了描述，包括：公司名称、注册地址、常用办公地点和相关负责人的联系方式等；
d) 隐私政策以单独成文的形式发布；
e) 隐私政策将收集个人信息的业务功能逐项列举，并逐一说明每个业务功能收集哪些个人信息类型；
f) 隐私政策中对个人敏感信息类型进行了显著标识；
g) 隐私政策中至少提供了一种投诉渠道；
h) 在用户安装、注册或首次开启政务应用时，主动提醒用户阅读隐私政策。当政务应用打开系统权限时，提示用户并说明该权限收集个人信息的目的。收集个人敏感信息时，通过弹窗提示等显著方式向用户明示收集、使用个人敏感信息的目的、方式、范围；
i) 未通过第三方SDK非法收集个人信息。

11.1.3.2 增强级

无。

11.1.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

11.2 安全保存检测方法

11.2.1 测试对象

政务应用、隐私政策文件、管理文档、数据管理员。

11.2.2 测试方法

11.2.2.1 基础级

a) 检查隐私政策文件，是否对个人信息存放地域（国内、国外）、存储期限、超期处理方式进行了明确说明；
b) 访谈数据管理员或检查管理文档，判断政务应用收集个人信息后，是否立即进行了去标识化处理，采取技术和管理方面的措施，将去标识化后的数据与可用于恢复识别的个人信息分开存储；
c) 检查政务应用，在传输和存储个人敏感信息时，是否采用了加密等安全措施；
d) 访谈数据管理员或检查管理文档，在存储个人生物识别信息时，是否采取技术措施处理后再进行存储，例如：仅存储个人生物识别信息的摘要；
e) 访谈数据管理员或检查管理文档，个人信息保存期限是否为实现目的所必需的最短时间；
f) 访谈数据管理员或检查管理文档，在政务应用停止运营时，是否及时停止继续收集个人信息的活动，将停止运营的通知逐一送达或公告的形式通知用户，对所持有的个人信息进行删除或匿名化处理。

11.2.2.2 增强级

无。

11.2.3 预期结果

11.2.3.1 基础级

a) 对个人信息存放地域（国内、国外）、存储期限、超期处理方式进行了明确说明；
b) 收集个人信息后，立即进行了去标识化处理，并采取技术和管理方面的措施，将去标识化后的数据与可用于恢复识别的个人信息分开存储；
c) 在传输和存储个人敏感信息时采用了加密等安全措施；
d) 在个人生物识别信息存储时采取了技术措施处理后再进行存储；
e) 个人信息保存期限设置为实现目的所必需的最短时间；
f) 在政务应用停止运营时及时停止继续收集个人信息的活动，将停止运营的通知逐一送达或公告的形式通知用户，对所持有的个人信息进行删除或匿名化处理。

11.2.3.2 增强级

无。

11.2.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

11.3 安全使用检测方法

11.3.1 测试对象

政务应用、隐私政策文件、数据管理员、管理文档。

11.3.2 测试方法

11.3.2.1 基础级

a) 访谈数据管理员或检查管理文档，判断政务应用是否遵循了最小化授权原则对个人信息采取访问控制措施；
b) 检查政务应用，对于需要通过界面展示个人信息的，是否对其采取了去标识化处理等措施；
c) 将个人信息用于用户画像、个性化展示等用途时，检查隐私政策中是否说明了其应用场景和可能对用户产生的影响；
d) 访谈数据管理员或检查管理文档，判断是否提供了查询、更正、删除个人信息的途径；
e) 检查政务应用，是否提供了注销账号的途径，如在线功能界面、客户电话等，并在用户注销账号后，及时删除其个人信息或进行匿名化处理；
f) 访谈数据管理员或检查管理文档，判断如果存在个人信息对外共享、转让、公开披露等情况，是否征得用户同意，检查隐私政策中是否明确了以下内容：
   1）对外共享、转让、公开披露个人信息的目的；
   2）涉及的个人信息类型；
   3）接收方类型或身份；
g) 如果存在个人信息出境情况，检查隐私政策中是否将出境个人信息类型逐项列出并显著标识，如字体加粗、标星号、下划线、斜体、颜色等。

11.3.2.2 增强级

无。

11.3.3 预期结果

11.3.3.1 基础级

a) 遵循了最小化授权原则对个人信息采取访问控制措施；
b) 对于需要通过界面展示个人信息的，采取了去标识化处理等措施；
c) 将个人信息用于用户画像、个性化展示等用途时，隐私政策中说明了其应用场景和可能对用户产生的影响；
d) 提供了查询、更正、删除个人信息的途径；
e) 提供了注销账号的途径，如在线功能界面、客户电话等，并在用户注销账号后，及时删除其个人信息或进行匿名化处理；
f) 如果存在个人信息对外共享、转让、公开披露等情况，在征得了用户同意的情况下进行，隐私政策中明确了以下内容：
   1）对外共享、转让、公开披露个人信息的目的；
   2）涉及的个人信息类型；
   3）接收方类型或身份；

g） 如果存在个人信息出境情况，隐私政策将出境个人信息类型逐项列出并显著标识。

11.3.3.2 增强级

无。

11.3.4 结果判定

上述预期结果满足基础级的判定为基本符合，在满足基础级要求的基础上满足增强级要求的判定为符合；其他情况判定为不符合。

附 录 A
（资料性附录）
政务应用 APP 威胁场景

A.1 应用界面劫持

Activity劫持（界面劫持）漏洞较为普遍，攻击者劫持目标Activity并制造跟目标Activity界面相似度很高的界面迷惑用户，恶意的开发者就可以对应程序进行攻击。对于有登陆界面的应用程序，他们可以伪造一个一模一样的界面，普通用户根本无法识别是真假。用户输入用户名和密码之后，恶意程序就可以悄无声息的把用户信息上传到服务器。

A.2 APP篡改

APP篡改是指在APP程序内添加或修改代码、替换资源文件、修改配置信息、更换图标、植入恶意代码等行为，再通过对篡改后的APP进行二次打包，生成各种盗版、钓鱼应用。

一些灰色产业链通过反编译市场上的APK文件，然后进行注入广告、内容篡改，再重新打包发布。利用该漏洞篡改的政务应用APP不仅无法为民众提供相应的政务服务，起不到政民互动的作用，而且还可能会传达失实甚至虚假的信息，这种行为在影响民众利益的同时还会影响政府甚至国家的形象。

A.3 敏感信息泄露

用户敏感信息泄露主要是因为信息未加密或储存位置不当造成的，如代码中明文使用敏感信息，数据库中明文保存敏感信息，通信过程中明文传输敏感信息，最终导致用户的账号、密码、手机号等重要信息泄露。典型的可能导致信息泄露的情形为使用明文HTTP进行数据传输。

A.4 漏洞利用

如果漏洞应用在支持在线个人业务办理的政务应用APP中，攻击者将可轻易获取用户的个人身份证号、身份证照片以及其他个人敏感信息，利用敏感信息形成黑产数据做非法盈利，或者通过植入色情类内容病毒进行恶意扣费，用户点击或者查看均在后台产生短信业务申请。严重危害个人利益，影响政府形象。