编号：CCRC-APPS-2024

移动互联网应用程序（App）
安全认证实施细则

2024-01-31发布　　2024-01

中国网络安全审查认证和市场监管大数据中

目 录

1. 适用范围

本细则适用于对移动互联网应用程序（以下简称“App”）的安全认证，认证对象主要指运行在移动智能终端上的应用程序，包括移动智能终端预置应用程序、下载安装的应用程序。

2. 认证依据

认证依据为GB/T 35273《信息安全技术 个人信息安全规范》中收集、使用用户信息的要求和GB/T 41391《信息安全技术 移动互联网应用程序（App）收集个人信息基本要求》以及国家行政主管部门发布的政策法规中涉及的要求。

上述标准应执行国家标准化行政主管部门发布的最新版本。

3. 认证模式

技术验证+初始现场审核+获证后监督

技术验证指由检测机构对认证对象是否符合标准条款要求进行的技术评价活动。通常情况下，在检测机构现场进行。

初始现场审核指由认证机构委派审核员对App运营情况是否符合标准条款要求进行的评价活动。通常情况下，在App运营的主要场所进行。

获证后监督指认证机构对获证App是否持续符合认证要求进行的评价活动。通常情况下，由认证机构组织实施，包括收集获证App质量信息，对获证App实施监测和检测等。

4. 认证实施程序

4.1. 认证委托及受理

4.1.1. 认证委托

认证委托人通常为通过App向用户提供服务的网络运营者，且取得市场监督管理部门或有关机构注册登记的法人资格。

认证委托人有下列情形之一的，认证机构不予受理认证委托：

(1) 违反国内相关法律法规，包括但不限于《网络安全法》《数据安全法》《个人信息保护法》；

(2) 在12个月内发生重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁的安全事件；

(3) 所持同类证书在撤销认证影响期内。

4.1.2. 申请资料

认证委托人提交的申请资料应包含以下内容：

(1) 认证申请书（模板）；

(2) 法人资格证明材料：营业执照/事业单位法人证/民办非企业单位登记证书和组织机构代码/统一社会信用代码的营业执照的复印件；

(3) App版本控制说明（模板）；

(4) 对认证要求符合性的自评价结果及证明文档（模板）；

(5) App名称、版本差异性说明（模板）；

(6) 认证委托人承诺书、认证委托授权书（模板）；

(7) App发布审批流程等制度性文档。

4.1.3. 认证单元的确定

认证机构按App名称、版本、操作系统划分认证单元。

同一认证单元内，操作系统是相同的，即App运行的移动操作系统是相同的；可以包含多个版本，一般主版本是相同的，不同收集、使用个人信息的目的、类型、方式是一致的。

同一认证单元发布在不同的渠道时需要认证委托人提交

4.1.4. 认证受理

认证机构对申请资料进行评审，于5天内根据评审结果向认证委托人发出受理通知或问题通知。

认证委托人收到受理通知，应在要求时限内确认App的技术验证版本。

认证委托人收到问题通知，应及时按要求进行整改。认证委托人在要求时限内未反馈改进情况，认证机构将终止认证委托，并向认证委托人发出通知。

4.2. 技术验证

4.2.1. 技术验证方案

认证机构收到认证委托人对于App技术验证版本反馈后，制定技术验证方案，向检测机构下达技术验证通知。

技术验证通知中明确样品要求、样品来源、依据标准、认证委托人信息等。

样品要求包括App的名称、版本、操作系统等。

样品来源根据认证委托人申请书中填写的内容确定，一般包括应用商店下载、认证委托人官网下载、认证委托人送样三种。样品由检测机构按照样品来源获取。

技术验证项目依据GB/T 35273《信息安全技术 个人信息安全规范》中收集、使用用户信息的要求和GB/T 41391《信息安全技术 移动互联网应用程序（App）收集个人信息基本要求》以及国家行政主管部门发布的政策法规中涉及的要求。

4.2.2. 技术验证实施

检测机构应对样品情况、技术验证过程作出完整记录，并保存、保密过程资料和样品，资料和样品应长期保存，确保样品追溯。

技术验证发现不符合时，检测机构向认证委托人出具不符合报告，并要求限期整改，整改期限（整改的累计时间）不超过60天，逾期未完成整改以及整改期限内仍不符合的，终止认证委托。

通常情况下，检测机构实施技术验证时间为30天。

4.2.3. 技术验证报告

认证机构制定统一的技术验证报告模板。

技术验证结束后，检测机构应向认证机构和认证委托人出具技术验证报告。

4.3. 现场审核

4.3.1. 依据标准

GB/T 35273《信息安全技术 个人信息安全规范》中个人信息安全事件处置、组织的个人信息安全管理要求和GB/T 41391《信息安全技术 移动互联网应用程序（App）收集个人信息基本要求》中第三方接入管理要求。

4.3.2. 现场审核实施

技术验证报告通过评审后，认证机构在5天内指定审核组，向认证委托人下达审核通知。

审核组制定审核计划，并与认证委托人协商确认审核时间。

审核组按照审核计划实施现场审核，发现不符合时，向认证委托人出具不符合报告，并要求限期整改，整改时间不超过30天，逾期未完成整改以及整改后仍不符合的，终止认证委托。

4.3.3. 现场审核报告

认证机构制定统一的现场审核报告模板。

现场审核结束后，审核组向认证委托人出具审核报告，提交规定的审核报告和原始记录文件。

4.4. 认证决定

认证机构对申请资料、技术验证结论、现场审核结论、复核结果和App行业监管发现问题的处置情况进行综合评价，做出认证决定。对符合认证要求的，认证委托人对认证证书信息及App信息确认后，认证机构颁发认证证书并允许使用认证标志；对不符合认证要求的，不予颁发认证证书，并通知认证委托人。

4.5. 获证后监督

4.5.1. 频次和方式

监督周期不大于12个月。

认证委托人至少每12个月进行自评价，并将自评价报告提交认证机构。

认证机构对获证App实施监督检查，监督方式包括日常监督和专项监督。

4.5.2. 认证委托人自评价

当出现如下情形时，认证委托人应在5天内按照认证机构提供的自评价报告模板提交自评价报告：

(1) 获证App隐私政策发生变化；

(2) 获证App收集、处理和使用个人信息的目的、类型、方式发生变化；

(3) 获证App运营者对所收集个人信息的共享、转让、公开披露的对象、方式和目的发生变化；

(4) 获证App运营者收到获证App个人信息保护相关的投

4.5.3. 日常监督

认证机构对获证App持续实施日常监督，日常监督内容包面：

(1) 获证App一致性检查；

(2) 获证App版本变更情况；

(3) 认证证书和认证标志的使用情况；

(4) 认证委托人开展自评价的情况；

(5) 获证App被行业通报、媒体曝光、网民举报投诉等情况；

(6) 获证App权限、隐私政策及相关SDK的情况。

日常监督发现不符合时，认证机构向认证委托人发出整改通知，要求限期整改，逾期未完成整改以及整改后仍不符合的，将视情形暂停或撤销认证证书。

认证机构每年度汇总监督情况，向认证委托人出具年度监督报告。

4.5.4. 专项监督

当出现如下情形，认证机构执行专项监督：

(1) 网民举报投诉、媒体曝光、行业通报等涉及获证App存在个人信息安全方面的问题，并经查实获证App运营者负有责任时；

(2) 获证App运营者因组织架构、服务模式等发生重大变更，或发生破产并购等可能影响App认证特性符合性时；

(3) 认证机构根据日常监督结果，对获证App与本规则中规定的标准要求的符合性提出具体质疑时；

(4) 主管部门对App启动个人信息保护相关的专项治理、专项检查等监管行动时。

认证机构应制定专项监督计划，确定专项监督中技术验证和/或现场审核的要求，向认证委托人发出专项监督通知，按计划对行综合评价。认证机构也可采取事先不通知的方式对获证Ap监督。

当出现上述（1）、（2）、（3）情形时，认证机构将视情形暂停或撤销认证证书。

4.5.5. 监督结果评价

认证机构对监督结果进行综合评价，做出认证决定。对符合认证要求的，可继续保持认证证书、使用认证标志。对不符合认证要求的，认证机构应当根据相应情形做出暂停或者撤销认证证书的处理。

5. 认证时限

认证时限是指自做出受理决定之日起至做出认证决定时所实际发生的工作日，一般为90个工作日（不包含整改时间）。技术验证时限和现场审核时限参照4.2和4.3的具体要求。

6. 认证证书

6.1. 证书的保持

认证证书有效期为3年。在有效期内，通过获证后监督保持认证证书的有效性。

认证证书有效期届满，需延续使用的，认证委托人应在认证证书有效期届满前90天内提出换证申请，认证机构受理换证申请，组织实施技术验证、现场审核后，做出认证决定，对符合认证要求的，换发认证证书，不符合认证要求的，将注销认证证书。

认证委托人在认证证书有效期届满时未提出换证申请，认证机构将注销认证证书。

6.2. 证书的变更

6.2.1. 变更申请

出现下列情况之一时，认证委托人应向认证机构提出变更照认证机构制定的模板填写变更申请书和变更差异说明：

(1) 获证App名称及版本变更；

(2) 认证委托人名称及注册地址发生变更；

(3) App运营者名称及运营地址发生变更；

(4) App研发者名称及注册地址发生变更；

(5) 认证依据标准、实施规则发生变更。

认证机构对变更申请及变更差异说明的内容进行评审，确定变更实施方案。出现（1）情况时，如差异说明中明确App发生个人信息收集、使用等方面的变化，应进行技术验证；出现（3）情况时，应进行现场审核；出现（5）情况时，应进行技术验证和现场审核。

6.2.2. 变更受理

认证机构对提交的变更申请资料进行评审，于5天内根据评审结果向认证委托人发出受理通知或问题通知。

6.2.3. 变更评价和批准

认证机构根据变更申请的内容，对提供的资料进行评价，如需进行技术验证和/或现场审核时，还应对技术验证结论和/或现场审核结论进行评价，做出认证决定。对符合变更要求的申请，认证机构批准其变更，颁发变更后的认证证书；不符合变更要求的申请，认证机构不予批准其变更或认证终止。

6.3. 证书的暂停

6.3.1. 暂停证书的条件

有下列情形之一的，认证机构组织审核评价，对符合暂停证书条件的，暂停认证证书：

(1) 获证App被主管部门通报、媒体曝光、网民举报投

(2) 获证后监督中发现App不能持续符合认证要求；

(3) App发生变更影响认证符合性时，未及时向认证机构报告变更情况；

(4) 认证委托人违规使用认证证书、认证标志；

(5) 认证标准或认证规则发生变化，认证委托人未按认证机构规定完成过渡转换；

(6) 认证委托人申请暂停认证证书。

6.3.2. 证书暂停的有关规定

(1) 认证证书暂停时，认证机构应通知认证委托人，告知证书暂停的原因和期限，明确恢复证书的要求，并予以公布。

(2) 证书暂停期间，认证委托人不得使用认证证书和认证标志。

(3) 暂停期限一般为180天，暂停时间自认证机构签发暂停通知书之日算起。

6.3.3. 证书的恢复

暂停期限内，认证委托人可提出恢复认证的申请。

认证委托人提交的恢复申请资料应包含以下内容：

(1) 恢复认证申请书；

(2) 暂停通知书中明确的恢复证书所需的资料要求。

认证机构对恢复申请资料进行综合评价，对符合要求的，恢复其认证证书，不符合要求的，认证机构不予批准其恢复。

6.4. 证书的撤销

6.4.1. 撤销证书的条件

有下列情形之一的，认证机构组织审核评价，对符合撤销的，撤销认证证书：

(1) 认证委托人、App运营者和App开发者存在个人信息的违法违规行为；

(2) 认证委托人、App运营者和App开发者存在欺骗、隐瞒、违反承诺等不当行为，影响认证有效性；

(3) 暂停到期，认证委托人未提交恢复申请或未采取有效整改措施。

6.4.2. 证书撤销的有关规定

(1) 认证证书撤销时，认证机构应通知认证委托人，并予以公布。

(2) 证书撤销后，认证委托人不得使用认证证书和认证标志。

6.5. 证书的注销

6.5.1. 注销证书的条件

有下列情形之一的，认证机构组织审核评价，对符合注销证书条件的，注销认证证书：

(1) 认证证书有效期届满，认证委托人未申请延续使用的；

(2) 认证委托人申请注销；

(3) 当认证委托人、App运营者和App开发者的经营主体已注销的。

6.5.2. 证书注销的有关规定

(1) 认证证书注销时，认证机构应通知认证委托人，并予以公布。

(2) 证书注销后，认证委托人不得使用认证证书和认证标志。

7. 认证证书和认证标志的使用和管理

7.1. 认证证书的使用和管理

认证证书有效期内，认证委托人可将证书在网站、工作场所和宣传资料中展示，但不应进行误导性宣传。

7.2. 认证标志的使用和管理

7.2.1. 认证标志的样式

认证标志样式由基本图案、认证机构识别信息组成。

图1 App安全认证标志

“CCRC”为中国网络安全审查认证和市场监管大数据中心机构识别信息。

认证标志可成比例放大或缩小，应清晰可辨。

7.2.2. 认证标志的使用和管理

认证委托人仅能在认证范围内使用认证标志，且和获证App同时使用，不应进行误导性宣传。

7.2.3. 认证标志的加施位置

通过认证的App应在下载页面及启动界面中以清晰、完整、显著的方式加施认证标志。

8. 收费

8.1. 收费标准

认证机构按对外公开的收费标准收取认证费用，收费标准可访问中国网络安全审查认证和市场监管大数据中心官网（www.iscc，信息公开——收费公示栏目查阅。

8.2. 收费原则

认证费用包括：申请费、批准与注册费、审核费、年金和技术验证费。

申请费为认证机构受理认证申请（包括初次申请、变更申请、证书到期延续申请和证书恢复申请等），进行申请评审所发生的费用，以认证单元为单位计费。

批准与注册费为认证机构复核，做出认证决定，批准颁发/换发/维持/恢复认证证书、制作发放认证证书等所发生的费用，以认证单元为单位计费。

审核费为认证机构实施现场审核所发生的费用，包含审核过程中所发生的交通和食宿费用，以人日为单位计费。

年金是证书有效期内每年度收取的一次性费用，为证书有效性管理、认证客户信息管理、获证App日常监督等所发生的费用，以认证单元为单位计费。

技术验证费为检测机构实施技术验证所发生的费用，按具体验证项目计费。

9. 认证责任

认证机构应对其做出的认证结论负责。

检测机构应对技术验证结果和技术验证报告负责。

认证机构及其所委派的审核员应对现场审核结论负责。

认证委托人应对其所提交的申请资料及样品的真实性、并对获证App持续符合认证要求负主体责任。

认证不能免除认证委托人对获证App承担的法律责任。