编号：CCRC-APPS-2019

移动互联网应用程序（App）
安全认证实施细则

2019-03-14发布　　2019-03-15实施

中国网络安全审查技术与认证中心

目　录

引言

移动互联网应用程序（App）安全认证实施细则（以下简称“实施细则”）是中国网络安全审查技术与认证中心根据国家认证认可监督管理委员会发布的CNCA-AppS-001《移动互联网应用程序（App）安全认证实施规则》的原则和要求，为细化实施要求和实施过程而制定的。

1 适用范围

本细则适用于针对具有收集、存储、传输和使用个人信息行为的移动互联网应用程序（以下称“App”）进行的数据安全认证。

2 认证依据

App安全认证的认证依据为GB/T 35273《信息安全技术 个人信息安全规范》及相关标准、规范。

上述标准原则上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

App安全认证的认证模式为：技术验证+现场审核+获证后监督。

4 认证程序

4.1 认证申请

4.1.1 申请方

认证申请主体为通过App向用户提供服务的网络运营者（以下简称“App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。

App运营者有下列情形之一的，不得申请认证：

（1）违反相关法律法规；

（2）在12个月内发生重大信息安全事件；

（3）所持同类证书在撤销认证影响期内；

（4）认证机构规定的其他情况。

4.1.2 申请单元的确定

原则上按App版本申请认证。同一名称的App，版本号、操作系统平台等不同时，一般应分为不同申请单元。

注1：一般情况下，App认证申请单元版本由主版本号、子版本号组成。特殊

情况下，另行确定认证对象版本的表述方式。

注 2：同一申请单元的 App 因版本号、发布渠道等原因导致存在差异的，认证申请方需提供版本间的差异性说明，并说明该差异与认证要求的关系。

4.1.3 申请方应提交的文件和资料

认证申请方在申请认证时，提交的文档资料应至少包含以下内容：

（1）认证申请书；

（2）法人资格证明材料；

（3）App版本控制说明；

（4）对认证要求符合性的自评价结果及相关证明文档；

（5）对App符合相关安全技术标准的证明文件；

（6）不同发布渠道的版本差异性说明；

（7）其他需要的文件。

4.2 认证受理

认证机构收到申请资料后，对申请资料的完整性、申请人主体资格进行评审，做出是否受理决定，并向认证申请方反馈受理决定。认证时限从认证受理之日开始计算。

资料评审一般不超过15个工作日。

4.3 技术验证

4.3.1 样本获取

认证申请方按照申请书填写的送样方式向认证机构提交样本，由认证机构将样本送交检测机构，并留存副本。

送样副本应反映所有发布渠道App副本与认证相关的技术特性；不能反映时，还应选送申请单元内其他App副本。

4.3.2 技术验证依据的标准

技术验证的依据为GB/T 35273《信息安全技术 个人信息安全规范》。

认证机构依据GB/T 35273《信息安全技术 个人信息安全规范》制定《移动互联网应用程序（App）安全评价指标》，明确技术验证的内容、方法和评价准则，作为技术验证的依据。

必要时，认证机构可要求检测机构按照相关技术标准对App的安全性进行验证。

4.3.3 技术验证方式

检测机构采用实验室检测和现场核查等方式进行。

4.3.4 技术验证实施

检测机构按照认证机构的安排，依据认证机构制定的《移动互联网应用程序（App）安全评价指标》实施技术验证，并按照认证机构规定的要求出具技术验证报告。

发现不符合项时，检测机构向认证申请方出具不符合报告，并要求限期整改；逾期未完成整改的，中止认证过程。

技术验证时间一般不超过30个工作日（自认证机构向检测机构下达任务之日起开始计算，整改和确认的时间不计算在内，一般不超过30个工作日）。

4.4 现场审核

认证机构对技术验证报告进行评审，做出评审结论。评审通过的，在30个工作日内完成现场审核；评审不通过的，视情况决定中止认证或要求检测机构重新出具技术验证报告。

4.4.1 现场审核依据的标准

现场审核依据的标准为GB/T 35273《信息安全技术 个人信息安全规范》。

认证机构依据GB/T 35273《信息安全技术 个人信息安全规范》制定《移动互联网应用程序（App）安全评价指标》，明确现场审核的内容、方法和评价准则。

4.4.2 现场审核实施

认证机构按照《移动互联网应用程序（App）安全评价指标》实施现场审核，并按照有关规定出具现场审核报告。

发现不符合时，认证机构向认证申请方出具不符合报告，并要求限期整改；逾期未完成整改的，中止认证过程。

4.5 认证决定

认证机构根据申请资料、技术验证结论和现场审核结论等进行综合评价，做出认证决定。认证决定通过后，由认证机构向认证申请方颁发认证证书，并授权获证App运营者使用规定的认证标志。认证决定不通过的，终止认证。

认证决定和批准时间、证书制作时间一般不超过15个工作日。

4.6 对认证决定的申诉

认证申请方如对认证决定结果有异议，可在收到认证结果通知后10个工作日内通过认证机构指定的申诉渠道进行申诉。认证机构自收

到申诉之日起，应在5个工作日内决定是否予以受理；对于受理的申诉，一般应在30个工作日内给出处理结果，并将处理结果书面通知认证申请方。

4.7 获证后监督

获证App运营者应持续进行获证后自评价，并配合认证机构的监督活动。

认证机构应对获证App和App运营者实施持续监督，监督方式包括日常监督和专项监督。

4.7.1 获证后自评价

获证App运营者应对获证App持续符合认证要求的情况进行自评价。当出现如下情形时，获证App运营者应向认证机构提交自评价报告：

（1）获证App的分发渠道发生变化；

（2）认证标志使用情况发生变化；

（3）获证App隐私政策发生变化；

（4）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；

（5）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；

（6）获证App运营者收到获证App个人信息保护相关的投诉举报。

4.7.2 日常监督

认证机构应对获证App和App运营者持续实施日常监督，日常监督的内容至少包括以下方面：

（1）获证App一致性检查；

（2）获证App的更新情况；

（3）认证证书和认证标志的使用情况；

（4）企业开展自评价的情况；

（5）获证App被网民举报投诉和社会媒体曝光情况；

（6）其他影响获证App在个人信息收集、处理和使用方面持续符合认证要求的情况。

认证机构应定期对日常监督情况进行评价，形成日常监督报告。

4.7.3 专项监督

当出现如下情形，认证机构应启动专项监督：

（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。

专项监督应对上述情形进行深入调查，并对获证App持续符合性进行全面审核，必要时还可进行技术验证。

认证机构可采取事先不通知的方式对获证App运营者实施专项监督。

4.7.4 监督结果的处理

获证后监督中发现不符合时，认证机构应要求获证App运营者在限期内进行整改，并对整改结果进行验证。未在规定期限内完成整改或整改结果未通过验证的，按照6.3规定处置。

5 认证时限

认证时限是指自做出受理决定之日起到做出认证决定时所实际发生的工作日，包括资料审核时间、技术验证时间、现场审核时间、认证决定和证书批准时间以及制作时间。认证时限一般为90个工作日（不包含整改时间）。

6 认证证书

6.1 证书的保持

认证证书的有效期为三年。证书有效期内，通过获证后的监督确保证书的有效性。当认证要求（如标准）发生变化时，应按规定期限换证，超过规定期限未换发的认证证书自行失效。

6.2 证书的变更

6.2.1 变更申请与通知

出现下列情况之一时，获证App运营者应向认证机构提出变更申请：

（1）获证App名称、版本发生变更；

（2）认证范围扩大或缩小；

（3）获证App运营者名称、注册地址发生变更；

（4）认证机构规定的其它事项发生变更时。

6.2.2 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，确定是否可以批准变更。如需重新技术验证和/或现场审核，应在技术验证和/或现场审核通过后方能批准变更。

6.3 认证的暂停、撤销和注销

6.3.1 暂停认证

有下列情形之一的，认证机构应暂停认证，并予以公布：

（1）国家有关主管部门发现获证App存在安全问题；

（2）在监督中发现获证App不能持续符合认证要求；

（3）获证App运营者在App发生重大变更后，未及时向认证机构报告变更情况；

（4）获证App运营者违规使用认证证书、认证标志；

（5）认证标准或认证规则发生变化，获证App运营者未按认证机构规定完成过渡转换；

（6）获证App运营者主动申请暂停认证；

（7）其他依法应当暂停的情形。

暂停期限一般为180天。暂停期限内，获证App运营者可提出恢复认证的申请，经认证机构审核、批准后，方可使用该证书。在暂停认证期间，获证App运营者不得继续使用证书和认证标志。

6.3.2 撤销认证

有下列情形之一的，认证机构应撤销认证，并予以公布：

（1）获证App运营者存在个人信息安全有关的违规违法行为；

（2）暂停认证期间，获证App运营者未采取有效整改措施；

（3）发现获证App运营者在认证过程中存在欺骗、隐瞒、违反承诺等不当行为，影响认证有效性；

（4）获证App运营者拒绝接受获证后监督；

（5）超过暂停期限；

（6）其他依法应当撤销的情形。

撤销认证后，获证App运营者应交回认证证书，停止使用认证标志。

6.3.3 注销认证

有下列情形之一的，认证机构应注销认证，并予以公布：

（1）获证App不再向用户提供服务；

（2）获证App运营者申请注销；

（3）其他依法应当注销的情形。

注销认证后，获证App运营者应交回认证证书，停止使用认证标志。

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

在认证证书的有效期内，获证App运营者可将证书在网站、工作场所和宣传资料中展示，但不应进行误导性宣传。

认证证书只能证明获证App在认证范围内的App数据安全符合了特定标准或其他引用文件，不能用来暗示其得到了认证机构的批准。

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技术与认证中心机构识别信息。

7.2.1.1 认证标志规格

认证标志的规格如图2所示，可成比例放大或缩小，应清晰可辨。

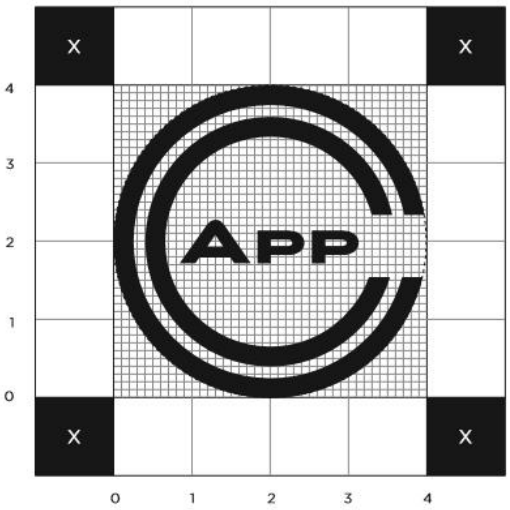

图2 认证标志规格图

7.2.1.2 认证标志颜色

认证标志的基本颜色为黑色。

黑色：C:0 M:0 Y:0 K:100（标准色）。

7.2.2 认证机构标识的样式

中国网络安全审查技术与认证中心标识样式如图3所示：

图3 认证机构标识样式

7.2.2.1 认证机构标识规格

认证机构标识的规格如图4所示，可成比例放大或缩小，应清晰可辨。

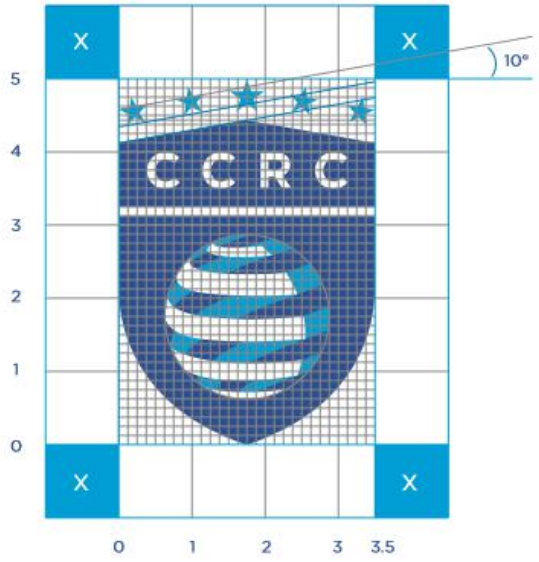

图4 认证机构标识规格图

7.2.2.2 认证机构标识颜色

认证机构标识的基本颜色为标准蓝、辅助蓝色。

蓝色： C:100 M:70 Y:0 K:0（标准色）；

辅助蓝色：C:100 M:0 Y:0 K:0（辅助色）。

7.2.3 认证标志的使用和管理

获证App运营者只能在认证范围内使用认证标志，且和获证App同时使用，不得单独使用，不应进行误导性宣传。

通过中国网络安全审查技术与认证中心认证的App使用认证标志时，可在其右侧加施认证机构标识。使用方式如下图5所示：

图5 认证标志与认证机构标识联合使用样式图

“XXX”用于表示认证属性的其它说明。

认证标志和机构标识的联合使用规格如下图6所示，在使用时可以在可辨识的条件下等比例的放大或缩小，不允许变形或变色。

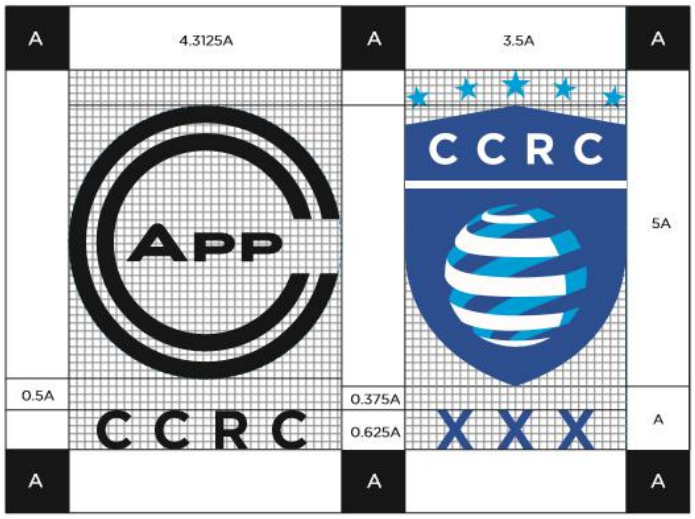

图6 认证标志与机构标识的联合使用规格图

被暂停或撤销（含注销）认证证书的，App运营者如果继续使用认证标志，认证机构有权要求其承担由此给认证机构造成的全部损失并承担法律责任。

7.2.4 认证标志的加施位置

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

8 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。

认证申请方（获证App运营者）应对其所提交的申请资料及样品的真实性、合法性负责，并对获证App持续符合认证要求负主体责任。

认证不能免除获证App运营者对获证App承担的法律责任。