附件

编号：CNCA-App-001

移动互联网应用程序（App）

安全认证实施规则

2019-03-13发布　　2019-03-15实施

国家认证认可监督管理委员会发布

目录

1 适用范围

本规则适用于对移动互联网应用程序（以下称“App”）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+现场核查+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，具体由认证机构依据本规则制定的认证实施细则予以规定。

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声明；

（7）其他需要的文件。

4.2 认证受理

认证机构对申请资料进行审核后做出受理决定，并向认证申请方反馈受理决定。

4.3 技术验证

4.3.1 样品获取

认证申请方按照申请书填写的送样方式提交样本。

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》。

认证机构应根据GB/T 35273制定技术验证规范，确定针对标准要求的技术验证内容、方法和评价准则。

4.3.3 技术验证方式

技术验证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

检测机构按照技术验证规范实施技术验证，并按照认证机构有关规定出具技术验证报告。

发现不符合时，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。

4.4 现场审核

技术验证通过后，认证机构对App运营者进行现场审核。

4.4.1 现场审核依据的标准

现场审核的依据为 GB/T 35273《信息安全技术个人信息安全规范》。

认证机构应根据 GB/T 35273 制定现场审核规范，确定针对标准要求的现场审核内容、方法和评价准则。

4.4.2 现场审核实施

认证机构按照现场审核规范实施现场审核，并按认证机构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。

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个工作日决定是否予以受理；对于受理的申诉，一般应在30个工作日给出处理结果，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发生变更，以及所引起的收集、处理和使用个人信息的目的、类型、方式发生变化；

（4）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；

（5）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

认证时限是指自作出受理决定之日起至作出认证决定所实际发生的工作日，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

认证机构应对认证证书的有效期做出规定，超过有效期的认证证书自行失效。当认证规则要求（如标准）发生变化时，应在认证机构确定的转换期限内完成换证。

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，认证机构经审核、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。

7.2 认证标志及其使用和管理

7.2.1 认证标志的式样

认证标志的式样由基本图案、认证机构识别信息组成。

A B C D

“ABCD”代表认证机构识别信息。

7.2.2 认证标志的使用和管理

认证机构应规定认证标志的使用和管理。

获证App运营者应按照认证机构的规定使用和管理认证标志，不得

进行误导性宣传。

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。