文件号	CEPREI-24-GM
版本号	1

CSA STAR Mobile

移动应用程序信息安全认证实施规则

广州赛宝认证中心服务有限公司

目　　录

1. 总则

1.1. 目的

为使申请方/受审核方/获证组织全面了解赛宝认证中心(以下简称本中心)受理并实施移动应用程序信息安全认证（以下简称 CSM 认证)的全过程，便于本中心有序、有效地开展 CSM 认证工作，保证 CSM 认证的工作质量，满足 CSA（Cloud Security Alliance）的授权要求，特制定本程序规则。

1.2. 适用范围

本程序规则适用于本中心开展的 CSM 认证工作，可为申请方/受审核方/获证组织进行 CSM 认证提供指导。

1.3. 主要依据文件

1）CSA 云安全联盟《移动应用安全测试标准》;

2）GB / T18336《信息技术 安全技术 信息技术安全性评估准则》

3）ISO/IEC 17065《产品、过程和服务认证机构要求》

4）ISO/IEC 17025《检测与校准实验室能力的通用要求》

上述文件中的条款通过本标准的引用而成为本标准的条款。凡是标注日期的引用文件，其随后所有的修改（不包括勘误的内容）或修订版均不适用于本标准，凡是不标注日期的引用文件，其最新版本适用于本标准。

1.4. 术语说明

根据认证过程的变化,本规则对申请认证单位使用了不同的称呼:

申请方：认证审核之前

受审核方：审核过程中及获证前

获证组织：获得 CSM 认证证书后。

1.5. 职责

管理委员会、技术委员会、各业务部门的职责与现在产品信息安全认证相同，但在具体的运作要求上，在开展 CSM 认证工作时，应遵循本计划的要求。

2. 申请方条件、责任和义务

2.1. 申请方应具备的基本条件

1) 持有法定登记注册证明，如独立法人地位证明文件等，如果申请方是大组织的一部分(无独立法人资格)，应持有大组织的授权证明等；

2) 认证申请组织应具备评价和保持法律法规符合性的机制，并按规定向有关部门及相关方通报所发现的不符合情况。

2.2. 申请方/受审核方的权利和义务

2.2.1 申请方/受审核方的权利

1) 自主选择咨询单位；

2) 与本中心协商确定认证时间；

3) 有权对本中心的认证活动等提出申诉/投诉和异议。

2.2.2 申请方/受审核方的义务

1) 按本中心要求提交申请文件及其附件；

2) 适用时，为本中心审核组调阅文件记录、安排被访问人员等提供必要的条件；

3) 保留顾客和/或相关方就获证组织的活动、产品或服务所提出的所有投诉记录，信息沟通记录及相应纠正措施记录，并在本中心要求时提供。重要投诉应及时通报赛宝认证中心；

4) 按规定及时交纳认证费用。

3. 认证的公正性

3.1. 管理委员会的组成

管理委员会的组成原则应遵循 CEPREI-01《管理委员会章程》的要求，无进一步要求，但专业能力应考虑移动应用产品信息安全的特殊性。

3.2. 评估结论决定人员的组成

相关要求参见 CEPREI-03《技术委员会工作细则》及 CEPREI-QP-14《认证决定程序》。CSM 认证评估结论决定人员的能力要求与 ISMS 体系一致，具体见《QP-48 ISMS 审核专业管理和审核员专业能力评定程序》。

4. 能力管理

4.1. 人员能力要求

CSM 认证涉及人员，如合同评审人员、评估方案管理人员、专业能力见证评价和专业培训指导人员、评估结论决定人员、专业评估师等的能力要求见《CSM 认证相关人员能力分析报告》和《CSM 认证审核员能力要求》。

4.2. 人员的选择与评价

CSM 认证业务对口管理部门依本中心文件 CEPREI-QP-02《人员录用、培训及监督程序》对该业务人员进行选择和评价。

4.3. 能力保持、提高及行为监视

除依据 CEPREI-QP-08《审核员管理程序》等程序实施能力保持提高及行为监视外，中心每年对 CSM 认证知识实施专题研讨培训，培训参与人员应覆盖 4.1 条所列人员；中心指定专人负责 CSM 认证信息及知识的收集，该负责人应负责整理相关信息并传递到 4.1 条所涉及人员，并识别培训需求，实施必要培训。

5. 认证程序

5.1. 认证模式

产品检测+认证+获证后的监督

委托人提出认证申请，赛宝先行就提交的申请材料进行资料审核。审核合格后，申请人与赛宝签订《CSA STAR Mobile 移动应用程序信息安全认证合同书》，由赛宝委托 CSA 认可的检测实验室（以下简称实验室）对移动应用程序（以下简称“APP”）进行信息安全检测。赛宝结合产品检测报告、配置管理、交付管理等材料进行文件审核，并可根据情况远程访谈受审核方人员及调阅文件记录。认证评价合格核发认证证书。证书有效期 3 年，证书保持通过年度监督维持。

5.2. 认证单元划分

按 APP 名称划分，相同委托人、相同开发商、相同版本（哈希值须一致）的 APP 认定为一个认证单元。

5.3. 认证决定人员管理

作为 CST 认证决定人员应特别强调如下条件：

1) CST 认证决定人员已经接受了 CST 认证的培训，并评价合格；

2) 具有专业的认证决定人员对评估结论决定具有否决权。

5.4. 认证申请提出和受理

市场拓展部依据 CEPREI-QP-06《合同管理程序》及 CEPREI-QP-11《认证申请受理程序》规定的步骤实施申请受理及合同评审，同时，还应由 CST 认证的合同评审人员进行评审。对申请方的要求如下：

1) CST 认证适用于所有移动应用程序，包括 IOS 和安卓平台产品；

2) 应提交《CSA STAR Mobile 移动应用程序信息安全认证申请书》及其附件。

5.5. 实施安排

赛宝在受理认证申请后，赛宝将认证实施方案通知认证申请方。认证实施方案通常包括如下内容：

（1） 需要提交的申请资料清单；

（2） 产品检测安排；

（3） 所需的认证流程及时限；

（4） 有关赛宝工作人员的联系方式；

（5） 其他需要说明的事项。

有关认证方案相应内容应告知认证申请方，明确相关内容及应履行的责任。

5.6. 认证的实施

5.6.1 基本要求

产品检测由实验室执行并出具检测报告，文件审核由赛宝执行。认证审核报告由赛宝出具。

5.6.2 产品检测

5.6.2.1 依据标准

依据 CSA《移动应用安全测试标准》

5.6.2.2 执行机构

由实验室对申请认证的 APP 执行检测

5.6.2.3 检测方式

由实验室组织开展检测。

5.6.2.4 检测结果出具

由实验室出具检测报告。

5.6.2.5 检测报告出具时限

实验室正式受理测试委托后 5 个工作日内完成产品检测并出具检测报告。

5.6.2.6 产品检测报告

测试组人员应如实记录产品检测的结果与数据，如有不符合条款，应详细说明不符合的情况。

5.6.3 文件审核

由赛宝对产品检测报告、产品配置管理、产品交付管理等材料进行文件审核，并可根据情况远程访谈受审核方人员及调阅文件记录。

5.6.3.1 审核内容

评估受审核方的配置管理能力、产品交付管理能力及产品一致性。

5.6.3.1.1 配置管理能力审核

重点核实以下内容：

- 受审核方应为产品提供一个参照号。
- 受审核方应使用一个配置管理系统。
- 受审核方应提供配置管理文档。
- 产品参照号对产品的每一个版本应是唯一的。
- 应该给产品标记上参照号。
- 配置管理文档应包括一个配置清单。
- 配置清单应唯一标识组成产品的所有配置项。
- 配置清单应描述组成产品的配置项。
- 配置管理文档应描述用于唯一标识产品所包含配置项的方法。
- 配置管理系统应唯一标识产品所包含的所有配置项。

5.6.3.1.2 产品交付能力审核

重点核实以下内容：

- 受审核方应制定并使用交付程序。
- 交付文档应描述，在向用户方分发产品版本时，用以维护其安全性所必需的所有程序。
- 受审核方应提供一个功能规范。
- 功能规范应使用非形式化风格来描述产品安全功能及其外部接口。

- 功能规范应是内在一致的。
- 功能规范应描述所有外部安全功能接口的用途与使用方法，适当时提供效果、例外情况和错误消息的细节。
- 功能规范应完备地表示产品安全功能。

5.6.3.1.3 产品一致性审核

重点核实以下内容：

1）认证产品的包装上所标明的及运行时所显示的产品名称、型号/版本与产品检测报告上所标明的内容是否一致；

2）认证产品所用的软件（含开源软件）与产品检测报告所列明的是否一致；

3）非认证的产品是否违规使用了认证标识。

5.6.4 不符合项处置

若评估审核过程中，产品检测和/或文件审核存在不符合项时，执行机构将不符合项内容进行记录，并告知受审核方不符合项的纠正时限与纠正验证方式，纠正措施采用书面整改或检测验证。原则上纠正时限不超过 30 个自然日，如无可接受原因，纠正时间超过 30 个自然日，则纠正措施无效。

5.6.5 评估报告的时限

审核组应在 5 个工作日内向赛宝提交 CSM 认证评估报告（以完成产品检测及文件审核并收到委托人提交的符合要求的不符合纠正措施报告之日起计算）。

5.6.6 评估报告结论

最终评估报告由产品检测结果与文件审核结果组成。评估结论分为“评估通过”、和“评估不通过”两种。

其中，“评估通过”指不存在不符合项，评估通过；“评估不通过”指审核结果存在不符合或纠正措施验证无效。

6. 认证结果的评定与批准

6.1. 认证结果和认证时限

赛宝应在审核组提交评估报告后完成认证评价。评价合格，通常在 5 个工作日内由赛宝向认证委托人颁发认证证书，认证证书为电子版。

评价不合格，则认证终止。

注：因委托人或需整改的时间不计算其中。

6.2. 认证暂停

由于产品检测的实际情况或委托人提出暂停申请等情况，可申请暂停认证过程。如需继续认证，委托人可提出恢复认证申请。如无可接受的原因，申请的暂停期不超过 12 个月。

6.3. 认证终止

因产品检测不通过、委托人提出撤销申请等原因，造成评价不通过或评价无法完成时，认证终止；因产品检测的不符合项未关闭、企业无法提供相关资料或纠正措施，且自申请受理之日起满 12 个月，认证终止。认证终止后如要继续申请认证，需重新提交申请，前期所提供资料或已完成的产品检测的全部或部分结果，将不作为重新申请的有效依据。

7. 认证证书

7.1. 证书的保持

认证证书有效期为 3 年。在有效期内，通过每年对获证后的产品进行监督确保认证证书的有效性。赛宝将应用市场中随机抽取认证范围内的 APP 送实验室检测，检测合格后，可以继续保持认证证书、使用认证标志。对监督时发现的不符合项应在 30 个自然日内完成纠正措施。逾期将撤销认证证书、停止使用认证标志，并对外公告。

7.2. 认证证书变更备案

7.2.1 变更的申请

获证后的产品，如果其生产厂商、证书持有者等发生变化时，应向认证机构提出变更申请。

7.2.2 变更申请的评价与批准

认证机构根据变更的内容和提供的资料进行审核后予以变更。

7.3. 认证证书的暂停、恢复、注销和撤销

证书的使用应符合《获证单位的权利、义务和证书、标志的使用说明》相关要求。如证书持证人违反证书管理相关规定，赛宝依据相关规定对证书做出相应的暂停、撤消和注销的处理，并将处理结果进行公告。证书持证人可以向赛宝申请暂停、注销其持有的证书。

证书暂停期间，证书持证人如需要恢复证书，应在证书暂停的期限内向赛宝提出恢复申请，赛宝按相关规定进行证书恢复。逾期未恢复的证书，赛宝依据相关规定撤消或注销被暂停的证书。

认证证书有效期内，如发生认证的相关 APP 被国家执法部门或行政主管部门下架的情况，则赛宝有权主动撤销认证证书而无需开发商同意。

7.4. 认证证书、认证标志的使用

7.4.1 认证证书和认证标志的使用

应符合《获证单位的权利、义务和证书、标志的使用说明》的要求。

认证标志在使用时可以等比例的放大或缩小，但是不允许变形或变色。

认证标志应加施在 APP 产品的适当位置，或 APP 产品的说明文档中。

7.4.2 APP 产品认证标志

图样见下图：

7.5. 认证产品变更

获证后的产品发生变更时，应以新版本产品向认证机构提出认证申请。

8. 收费

按《赛宝 CSA STAR Mobile 移动应用程序信息安全认证收费标准》收费。

9. 认证责任

赛宝对做出的认证决定负责。

赛宝对审核结果和审核报告负责。

实验室对产品检测结果和产品检测报告负责。

申请方应对其所提交的委托资料的真实性、合法性负责。

10. 技术争议及申诉

申请方提出的申诉、投诉和争议按照赛宝的相关规定处理。

11. 信息公开

见赛宝网站 www.ceprei.org。