

编号：ISCCC-IR-002:2011

IT 产品信息安全认证实施规则 操作系统安全加固产品

2011-07-01 发布

2011-07-01 实施

中国信息安全认证中心发布

目 录

1. 适用范围	1
2. 认证模式	1
3. 认证的基本环节.....	1
3.1 认证申请及受理	1
3.2 文档审核	1
3.3 型式试验委托及实施.....	1
3.4 初始工厂检查（如适用）	1
3.5 认证结果评价与批准.....	1
3.6 获证后监督	1
4. 认证实施	1
4.1 认证流程	1
4.2 认证申请及受理	1
4.3 文档审核	3
4.4 型式试验委托及实施.....	3
4.5 初始工厂检查（如适用）	3
4.6 认证结果评价与批准.....	4
4.7 获证后监督	4
5. 认证时限	5
6. 认证证书	6
6.1 认证证书的保持	6
6.2 认证证书的变更	6
6.3 认证证书覆盖产品的扩展.....	6
6.4 认证证书的暂停、注销和撤销.....	6
7 认证标志的使用	7
7.1 认证标志的样式	7
7.2 认证标志的使用	7
7.3 加施方式	7
7.4 标志位置	7
8 收费	7
附件 1:	8
附件 2:	10

1. 适用范围

本规则所指的操作系统安全加固产品是指通过自主可控的安全技术对操作系统产品的安全性进行增强，提高对其本身以及系统内私人信息的正确控制，以降低未经授权更改、不必要的或无保证的传播或遗失的可能性或损失的操作系统类信息安全产品。

本规则适用的产品范围为：以操作系统安全加固功能为主体的软件或软硬件组合。

2. 认证模式

型式试验 + 初始工厂检查（如适用）+ 获证后监督

3. 认证的基本环节

3.1 认证申请及受理

3.2 文档审核

3.3 型式试验委托及实施

3.4 初始工厂检查（如适用）

3.5 认证结果评价与批准

3.6 获证后监督

4. 认证实施

4.1 认证流程

申请方向认证机构申请认证，认证机构在接收到申请方的认证申请后，审查申请资料，确认合格后向申请方选择的实验室安排检测任务，并通知申请方根据要求送样。实验室依据相关标准和/或技术规范进行检测，并在完成检测后向认证机构提交检测报告。认证机构对检测报告审查合格后，需要时由认证机构组织进行初始工厂检查。认证机构对型式试验、初始工厂检查结果（如适用）进行综合评价，并在认证决定评价合格后向申请方颁发认证证书。认证机构组织对获证后的产品进行定期的监督。

4.2 认证申请及受理

申请方向认证机构递交认证申请，并按要求提交相关资料，认证机构对资料进行初审，确定申请方提交资料满足要求后，受理该申请。

4.2.1 认证的单元划分

原则上按产品型号/版本申请认证。

4.2.2 申请资料要求

申请方在申请产品认证时，应至少提交以下资料：

1) 申请基本信息：

- 认证申请书；
- 申请方声明；
- 相关法律地位证明材料（复印件）；
- 质量体系方面有关的文件。

2) 产品相关说明：

- 中文产品功能说明书和/或使用手册；
- 认证标准的适应性说明；
- 产品研制主要技术人员情况表；
- 产品测试技术人员情况表；
- 产品测试使用的主要设备表（如适用）；
- 中文铭牌和警告标记（如适用）；
- 产品密码检测合格证书（如适用）。

3) 安全保证要求方面的文档：

- 配置管理；
- 交付与运行；
- 开发；
- 指导性文档；
- 测试；
- 脆弱性评定。

4) 安全目标（如适用）。

4.3 文档审核

对申请方提交的资料和文档，根据相关标准和/或该产品的技术规范进行审核。

4.4 型式试验委托及实施

4.4.1 型式试验送样

4.4.1.1 送样原则

送申请认证的型号/版本的样品。

申请方如果有特殊要求，需要提供相应的说明及辅助设备。

4.4.1.2 送样要求和数量

用于检测的样品由申请方负责按上述要求选送，并对选送样品负责。一般每种产品送样 2 套，如果特殊需求可以增加送样数量。

4.4.1.3 样品及相关资料的处置

认证结束后，申请方可向实验室申请取回型式试验样品，相关申请资料由认证机构、实验室妥善处置。

4.4.2 检测依据

GB/T 18336-2008 《信息技术 安全技术 信息技术安全性评估准则》

ISCCC-TR-001-2011 《操作系统安全加固产品安全技术要求》

4.4.3 检测报告的提交

检测完成后，检测实验室根据认证机构的要求出具检测报告并提交给认证机构。

4.5 初始工厂检查（如适用）

4.5.1 检查内容

初始工厂检查的内容为信息安全保证能力、质量保证能力和产品一致性检查。

4.5.1.1 信息安全保证能力检查

由认证机构派检查员对工厂按照附件 2（信息安全保证能力评估项目）进行信息安全保证能力检查。

4.5.1.2 质量保证能力检查

由认证机构派检查员对工厂按照附件 1（质量保证能力基本要求）及认证机构制定的补充检查要求（适用时）进行检查。

4.5.1.3 产品一致性检查

初始工厂检查时，应在生产现场对申请认证的产品进行一致性检查。重点核实以下内容：

- 1) 认证产品的铭牌、包装上所标明的及运行时所显示的产品名称、型号/版本号与型式试验报告上所标明的内容是否一致；
- 2) 认证产品所用的软件、硬件应与型式试验合格的样品一致；
- 3) 非认证的产品是否违规标贴了认证标识。

4.5.2 初始工厂检查时间

一般情况下,认证机构对 4.2.2 中的资料进行审查并在型式试验完成后,再进行初始工厂检查。特殊情况时,型式试验和初始工厂检查也可以同时进行。

初始工厂检查时间根据所申请认证产品的单元数量确定,并适当考虑生产厂的规模及产品的安全级别,一般每个生产厂为 2 至 6 个人日。

4.6 认证结果评价与批准

认证机构负责对型式试验结果等进行综合评价,评价合格的,由认证机构对申请方颁发认证证书(每一个认证单元颁发一个认证证书)。如认证决定过程中发现不符合认证要求项,允许限期(不超过 3 个月)整改,如期完成整改后,认证机构采取适当方式对整改结果进行确认,重新执行认证决定过程。

4.7 获证后监督

4.7.1 监督的频次

从获证后每 12 个月进行一次获证后监督。必要时，认证机构可采取事先不通知的方式进行必要的监督。

如果发生下述情况之一可增加监督频次：

1) 获证产品出现严重质量问题时，或者用户提出投诉并经查实为证书持有者责任时；

2) 认证机构有足够理由对获证产品与规定的标准要求符合性提出质疑时；

3) 有足够信息表明工厂因组织机构、生产条件、质量管理体系等发生变更，从而可能影响产品质量时。

4.7.2 监督的内容

获证后监督采用工厂检查的方式进行，主要针对信息安全保证能力、认证产品一致性和质量保证能力进行检查。必要时可以抽取样品送实验室检测，需要进行抽样检测时，抽样检测的样品应在工厂生产的产品中（包括生产线、仓库、市场）随机抽取。产品抽样检测的数量为 2 套，如可以根据实际情况增加抽样的数量。初次认证申请时的检测项目都可以作为监督时的检测项目，认证机构可根据具体情况进行部分或全部项目的检测。样品的检测一般由认证机构指定的检测实验室在 20 个工作日内完成。

4.7.3 获证后监督结果的评价

监督复查合格后，可以继续保持认证证书、使用认证标志。对监督复查时发现的不符合项应在 3 个月内完成纠正措施。逾期将撤销认证证书、停止使用认证标志，并对外公告。

5. 认证时限

认证时限是指自申请被正式受理之日起至颁发认证证书时止所实际发生的工作日，一般在 90 个工作日内，最长不超过 150 个工作日。整改时间不计算在内。

6. 认证证书

6.1 认证证书的保持

6.1.1 证书的有效性

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。

6.2 认证证书的变更

6.2.1 变更的申请

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

6.2.2 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。

6.2.3 证书的有效期

证书在进行变更后，其有效期与原证书一致。

6.3 认证证书覆盖产品的扩展

6.3.1 认证证书覆盖产品扩展申请

认证证书持有者需要增加已经获得认证产品的认证范围时，应向认证机构提出扩展申请，并提交扩展产品和原认证产品之间的差异说明。

6.3.2 认证证书覆盖产品扩展的评价与批准

认证机构应核查扩展产品与原认证产品的一致性，确认原认证结果对扩展产品的有效性，需要时应针对差异做补充检测，并根据认证证书持有者的要求单独颁发认证证书或换发认证证书。

6.3.3 证书的有效期

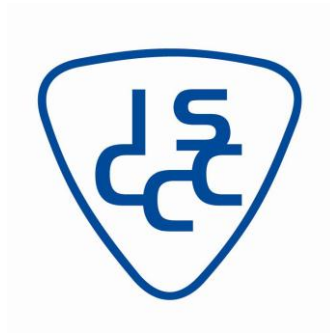
证书在进行扩展后，其有效期与原证书一致。

6.4 认证证书的暂停、注销和撤销

按认证机构的认证暂停、注销和撤销的相关规定执行。

7 认证标志的使用

7.1 认证标志的样式



7.2 认证标志的使用

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。

7.3 加施方式

采用认证机构印制的标准规格标志。

7.4 标志位置

应在产品本体的铭牌附近加施认证标志。

软件产品应在其软件包装/载体上加施认证标志，如该软件产品不使用包装/载体，则应在软件使用的《许可协议》中的显著位置明确该产品已获认证机构认证。

8 收费

收费由认证机构依据国家有关规定统一收取。

附件 1:

质量保证能力基本要求

为保证批量生产的认证产品与型式试验样品的一致性，工厂应满足本文件规定的质量保证能力基本要求。

1. 职责和资源

1.1 职责

工厂应规定与质量活动有关的各类人员职责及相互关系，且工厂应在组织内指定一名质量负责人，无论该成员在其他方面的职责如何，应具有以下方面的职责和权限：

- a) 负责建立满足本文件要求的质量体系，并确保其实施和保持；
- b) 确保加贴认证标志的产品符合认证标准的要求；
- c) 建立文件化的程序，确保认证标志的妥善保管和使用；
- d) 建立文件化的程序，确保不合格品和获证产品变更后未经认证机构确认，不加贴认证标志。

质量负责人应具有充分的能力胜任本职工作。

1.2 资源

工厂应配备必须的生产设备和检测设备以满足稳定生产符合本规则中规定的标准要求的产品；应配备相应的人力资源，确保从事对产品质量有影响工作的人员具备必要的能力；建立并保持适宜产品生产、试验、储存等必备的环境。

2. 认证产品一致性

a) 工厂应对现场的产品与型式试验样品的一致性进行控制，以使认证产品持续符合规定的要求；

b) 工厂应建立产品变更控制程序，认证产品的变更在实施前应向认证机构申报并获得批准后方可执行。

3. 认证产品外购部件或外包软件模块管理

3.1 外购部件供应商或软件模块的外包商的控制

a) 工厂应制定外购部件供应商或软件模块外包商的选择、评定和日常管理的程序，以确保供应商提供的部件或软件外包商提供的软件模块满足要求；

b) 工厂应保存对供应商或软件外包商的选择评价和日常管理记录。

3.2 外购部件或外包软件模块的验证

a) 工厂应建立并保持对供应商提供的部件或软件外包商提供的软件模块的验证程序及定期确认程序，以确保部件或软件模块满足认证所规定的要求；

b) 工厂应保存部件或外包软件模块，或者它们的验证记录、确认记录及供应商或软件外包商提供的合格证明及有关数据等。

附件 2:

信息安全保证能力评估项目

1. 配置管理

1.1 配置管理能力

- 开发者应为产品提供一个参照号。
- 开发者应使用一个配置管理系统。
- 开发者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。

2. 交付与运行

2.1 交付

- 开发者应将把产品或其部分交付给用户的程序文档化。
- 开发者应使用交付程序。
- 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。

2.2 安装、生成和启动

- 开发者应将产品安全地安装、生成和启动必需的程序文档化。
- 安装、生成和启动文档应描述产品安全地安装、生成和启动必需的所有步骤。

3. 开发

3.1 功能规范

- 开发者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。

3.2 高层设计

- 开发者应提供产品安全功能的高层设计。
- 高层设计的表示应是非形式化的。
- 高层设计应是内在一致的。
- 高层设计应按子系统描述安全功能的结构。
- 高层设计应描述每个安全功能子系统所提供的安全功能性。
- 高层设计应标识安全功能所要求的任何基础性硬件、固件或软件，以及在這些硬件、固件或软件中实现的支持性保护机制所提供功能的一个表示。
- 高层设计应标识安全功能子系统的所有接口。
- 高层设计应标识安全功能子系统的哪些接口是外部可见的。

3.3 表示对应性

- 开发者应提供一个所提供安全功能表示的所有相邻对之间对应性的分析。
- 对于所提供安全功能表示的每个相邻对，分析应证实，较为抽象的安全功能表示的所有相关安全功能都在较不抽象的安全功能表示中得到正确且完备地细化。

4. 指导性文档

4.1 管理员指南

- 开发者应提供针对系统管理员的管理员指南。
- 管理员指南应描述产品管理员可使用的管理功能和接口。
- 管理员指南应描述如何以安全的方式管理产品。
- 管理员指南应包含一些关于安全处理环境中应被控制的功能和特权的警示信息。
- 管理员指南应描述所有关于与产品安全运行有关用户行为的假设。
- 管理员指南应描述所有受管理员控制的安全参数，适当时应指明安全值。
- 管理员指南应描述每一种与需要执行的管理功能有关的安全相关事件，包括改变安全功能所控制实体的安全特性。
- 管理员指南应与供评估的所有其他文档保持一致。
- 管理员指南应描述所有与管理员有关的 IT 环境安全要求。

4.2 用户指南

- 开发者应提供用户指南。
- 用户指南应描述产品的非管理员用户可使用的功能和接口。
- 用户指南应描述产品所提供的用户可访问安全功能的使用。
- 用户指南应包含一些关于安全处理环境中应被控制的用户可访问功能和特权的警示信息。
- 用户指南应清晰地阐述产品安全运行所必需的所有用户职责，包括与产品安全环境陈述中可找到的与关于用户行为的假设有关的那些职责。
- 用户指南应与供评估的所有其它文档保持一致。
- 用户指南应描述所有与用户有关的 IT 环境安全要求。

5. 测试

5.1 覆盖范围

- 开发者应提供测试覆盖的证据。

- 测试覆盖的证据应说明测试文档中所标识的测试与功能规范中所描述的安全功能之间的对应性。

5.2 功能测试

- 开发者应测试安全功能，并文档化测试结果。
- 开发者应提供测试文档。
- 测试文档应包括测试计划、测试程序描述、预期的测试结果和实际的测试结果。
- 测试计划应标识要测试的安全功能和描述要执行的测试的目标。
- 测试程序描述应标识要执行的测试和描述每个安全功能的测试脚本。这些脚本应包括对于其它测试结果的任何顺序依赖性。
- 预期的测试结果应指出测试成功执行后的预期输出。
- 开发者执行测试所得到的测试结果应证实每个被测试的安全性功能都按照规定运转。

5.3 独立性测试

- 开发者应提供用于测试的产品。
- 产品应适合测试。

6. 脆弱性评定

6.1 安全功能强度

- 开发者应对安全目标中所标识的每个具有产品安全功能强度声明的安全机制进行产品安全功能强度分析。
- 对于每个具有产品安全功能强度声明的安全机制，产品安全功能强度分析应说明该机制达到或超过安全目标中定义的最低强度级别。
- 对于每个具有特定产品安全功能强度声明的安全机制，产品安全功能强度分析应说明该机制达到或超过安全目标中定义的特定功能强度度量。

6.2 脆弱性分析

- 开发者应执行脆弱性分析。
- 开发者应提供脆弱性分析文档。
- 脆弱性分析文档应描述为搜索用户能违反安全策略的明显方法而执行的产品可交付材料分析。
- 脆弱性分析文档应描述对明显的脆弱性的处置。
- 脆弱性分析文档应针对所有已标识的脆弱性，说明脆弱性不能在产品的预期使用环境中被利用。