编号：ISCCC-IR-033:2017

IT 产品信息安全认证实施规则

评估保障级（EAL）

2017-08-14 发布　　2017-08-14 实施

中国信息安全认证中心发布

目 录

1．适用范围

本规则适用于中国信息安全认证中心（ISCCC）针对信息技术产品开展的基于评估保障级（EAL）的信息安全认证。

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 检测评估

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和评估，并在完成检测后向认证机构提交型式试验报告。认证机构对型式试验报告审查合格后，需要时由认证机构组织进行初始工厂检查。完成初始工厂检查后，实验室向认证机构提交评估技术报告。

认证机构对检测结果、初始工厂检查（如适用）和评估结果进行综合评价，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 认证单元划分

原则上按产品型号/版本申请认证。如果不同型号/版本之间的差异不影响产品满足标准的要求，可作为一个认证单元申请认证。

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）。

2） 产品相关说明：

- 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）；
- 同一认证单元中不同产品间的差异说明（如适用）；
- 产品密码检测合格证书（如适用）。

3） 安全保障要求方面的文档：

- 开发；
- 指导性文档；
- 生命周期支持；
- 安全目标
- 测试；
- 脆弱性评定（如适用）。

上述文档参考《EAL1-EAL5 级认证评估文档编写指南》和《EAL1-EAL5 级 ST 文档编写指南》编制。

4.3 文档审核

认证机构对申请方提交的资料和文档，根据相关标准和/或技术规范进行审核。

4.4 检测评估

4.4.1 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，根据检测的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《信息技术 安全技术 信息技术安全评估准则》、具体产品对应 EAL 级别的安全技术要求等。

4.4.3 型式试验报告的提交

检测完成后，实验室根据认证机构的要求出具型式试验报告并提交给认证机构。

4.4.4 评估技术报告的提交

检测和初始工厂检查（如适用）完成后，实验室根据认证机构的要求出具评估技术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障能力、质量保证能力和产品一致

性检查。

4.5.1.1 信息安全保障能力检查

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

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（如适用）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，具体人日数视实际情况酌情确定。

4.6 认证结果评价与批准

认证机构依据检测结果、初始工厂检查及评估结果，以及申请方提交的相关资料进行认证决定，决定是否颁发认证证书：

1） 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）。

2） 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。

3） 评价为不合格的，与申请方协商并处理后仍不能达到要求，不予颁发认证证书，并通知申请方原因。

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的符合性提出质疑时；

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

获证后监督通常采用提交证明材料或工厂检查的方式进行，EAL1 级别产品的监督一般采用提交证明材料的方式，必要时采用工厂检查的方式，EAL2 以上级别（包括 EAL2 级别）产品的监督均采用工厂检查的方式。工厂检查主要针对信息安全保障能力、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一般与初次申请认证进行测评时的数量一致，如需要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，一般为 90 至 180 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

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。

6.5 获证产品名录的发布

认证机构按相关规定对外公布获证产品的信息，包括：

- 产品名称、型号、版本；
- 认证委托人名称、地址；
- 认证依据的标准、规范；
- 发证日期及证书状态。

7 认证标志的使用

7.1 认证标志的样式

X 表示信息安全认证有关评估保障级别对应的数字，取值为“1”、“2”、“3”、“4”或者“5”。

7.2 加施位置

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

认证费用依据国家有关规定收取。

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：

信息安全保障能力工厂检查项目

保障级别	保障类	保障组件
EAL1	ALC：生命周期支持	TOE标识（ALC_CMC.1）
		TOE CM覆盖 （ALC_CMS.1）
EAL2	ALC：生命周期支持	CM系统的使用（ALC_CMC.2）
		部分TOE CM覆盖（ALC_CMS.2）
		交付程序（ALC_DEL.1 ）
EAL3	ALC：生命周期支持	授权控制 （ALC_CMC.3 ）
		实现表示CM覆盖 （ALC_CMS.3 ）
		交付程序（ALC_DEL.1 ）
		安全措施标识（ALC_DVS.1 ）
EAL4	ALC：生命周期支持	生产支持和接受程序及其自动化（ALC_CMC.4）
		问题跟踪CM覆盖 （ALC_CMS.4 ）
		交付程序（ALC_DEL.1 ）
		安全措施标识（ALC_DVS.1）
EAL5	ALC：生命周期支持	生产支持和接受程序及其自动化（ALC_CMC.4 ）
		开发工具CM覆盖 （ALC_CMS.5）
		交付程序（ALC_DEL.1）
		安全措施标识（ALC_DVS.1）

上述保障组件的具体内容参见GB/T 18336.3《信息技术　安全技术　信息技术安全评估准则 第3部分：安全保障组件》。