

编号：CNCA-CCIS-2018

网络关键设备和网络安全专用产品 安全认证实施规则

国家认证认可监督管理委员会发布

目 录

1. 适用范围	4
2. 认证模式	4
3. 认证的基本环节	4
3.1 认证申请及受理	4
3.2 文档审核	4
3.3 型式试验委托及实施	4
3.4 工厂检查	4
3.5 认证结果评价与批准	4
3.6 获证后监督	4
4. 认证实施	4
4.1 认证流程	4
4.2 认证申请及受理	5
4.3 文档审核	7
4.4 型式试验委托及实施	7
4.5 工厂检查	8
4.6 认证结果评价与批准	9
4.7 获证后监督	9
5. 认证时限	10
6. 认证证书	11
6.1 证书的有效性	11
6.2 认证证书的变更	11
6.3 认证证书覆盖产品的扩展	11
6.4 认证证书的暂停、注销和撤销	12
7. 认证标志的使用	12
7.1 认证标志的样式	12

7.2 认证标志的使用..... 12

7.3 加施方式..... 12

7.4 标志位置..... 13

附件 1： 14

附件 2： 16

附件 3： 17

1.适用范围

本规则依据《中华人民共和国网络安全法》《中华人民共和国认证认可条例》制定，规定了开展网络关键设备和网络安全专用产品安全认证的基本原则和要求。

本规则适用的网络关键设备和网络安全专用产品，应符合《国家互联网信息办公室、工业和信息化部、公安部、国家认监委关于发布<网络关键设备和网络安全专用产品目录（第一批）>的公告》（联合公告 2017 年第 1 号）中相应的范围要求描述（详见附件 1）。

安全认证用标准依据有关主管部门的要求执行。

2.认证模式

型式试验 + 工厂检查 + 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 工厂检查

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

认证委托人向认证机构申请认证, 认证机构在接收到认证委托人的认证申请后, 审查申请资料, 确认合格后向认证委托人选择的实验室安排检测任务, 并通知认证委托人根据要求抽样检测。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工厂检查。认证机构对型式试验、工厂检查结果进行认证决定, 并在认证决定评价合格后向认证委托人颁发认证证书。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

认证委托人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, 确定认证委托人提交资料满足要求后, 受理该申请。

4.2.1 认证的单元划分

按产品型号/版本申请认证, 若产品的关键件相同的可作为一个单元申请认证, 由认证机构根据认证要求对产品关键件做出规定。

以多于一个型号/版本的产品为同一认证单元申请认证时, 认证委托人应提交同一认证单元中型号/版本间的差异说明及相关测试报告。

4.2.2 申请资料要求

认证委托人在申请安全认证时，应至少提交以下资料：

1) 申请基本信息：

- 认证申请书；
- 认证委托人声明；
- 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) 有关技术指标参数声明及支撑材料（依据附件 1“范围”中的内容）。

3) 产品相关说明：

- 中文产品功能说明书和/或使用手册；
- 认证标准的适用性说明；
- 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；
- 中文铭牌和警告标记；
- 同一认证单元中型号/版本间的差异说明及相关测试报告（如适用）；
- 产品密码检测合格证书（如适用）。

4) 安全保障要求方面的文档：

- 配置管理；
- 交付与运行；

- 开发；
- 指导性文档；
- 测试。

5) 安全功能相关说明文件。

6) 认证机构要求的其他资料。

4.3 文档审核

对认证委托人提交的资料和文档，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 型式试验抽样

4.4.1.1 抽样要求

由认证机构安排对申请认证的产品按型号/版本进行抽样，样品应在生产企业生产的产品中（包括生产线、仓库、市场）随机抽取。一般每种产品抽样 2 套，如有特殊需求可增加样品数量。

认证委托人将样品递送至实验室，并对样品负责。

认证委托人应根据型式试验的要求，提供相应的说明及辅助设备。

4.4.1.2 样品及相关资料的处置

认证结束后，认证委托人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 型式试验依据

按相应产品有关国家标准的要求执行。

4.4.3 型式试验报告的提交

型式试验完成后, 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。

4.5 工厂检查

4.5.1 审核内容

工厂检查的内容为信息安全保障能力、质量保证能力、产品一致性检查。

4.5.1.1 信息安全保障能力

由认证机构派检查员对制造商、生产企业按照附件 2（信息安全保障能力基本要求）实施审核（当认证依据的国家标准涵盖安全保障能力要求时，则按相应国家标准实施）。

4.5.1.2 质量保证能力

由认证机构派检查员对生产企业按照附件 3（质量保证能力基本要求）及认证机构制定的补充检查要求进行检查。

4.5.1.3 产品一致性

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。重点检查以下内容:

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 工厂检查时间

由认证机构根据认证实施需要安排工厂检查。人日数根据所申请认证产品的单元数量确定，并适当考虑制造商、生产企业的规模及产品的安全级别，一般每个场所为 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、工厂检查结果等进行综合评价，做出认证决定，通过认证决定的，由认证机构对认证委托人颁发认证证书（每一个认证单元颁发一张认证证书）。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

监督频次一般为一年一次，当有特别规定时，认证机构可调整监督频次。必要时，认证机构可采取事先不通知的方式进行监督。

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) 有足够信息表明制造商、生产企业因组织机构、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，按 4.4.1.1 要求实施抽样。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。整改时间不计算在内。

6.认证证书

6.1 证书的有效性

证书有效期 5 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，如果其制造商、生产企业、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文件审核，需要时安排型式试验和/或工厂检查，认证评价通过后予以变更证书。

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型式试验

和/或工厂检查，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

参照《强制性产品认证证书注销、暂停、撤销实施规则》的要求执行。在认证证书暂停期间及认证证书注销和撤销后，获证机构不得使用证书。

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

可以采用统一印制的标准规格标志、模压、铭牌印刷、软件加施等方式。

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。

附件 1

网络关键设备和网络安全专用产品目录

	设备或产品类别	范围
网络关键设备	1. 路由器	整系统吞吐量（双向）≥12Tbps 整系统路由表容量≥55万条
	2. 交换机	整系统吞吐量（双向）≥30Tbps 整系统包转发率≥10Gpps
	3. 服务器（机架式）	CPU数量≥8个 单CPU内核数≥14个 内存容量≥256GB
	4. 可编程逻辑控制器（PLC 设备）	控制器指令执行时间≤0.08微秒
网络安全专用产品	5. 数据备份一体机	备份容量≥20T 备份速度≥60MB/s 备份时间间隔≤1小时
	6. 防火墙（硬件）	整机吞吐量≥80Gbps 最大并发连接数≥300万 每秒新建连接数≥25万
	7. WEB 应用防火墙（WAF）	整机应用吞吐量≥6Gbps 最大HTTP并发连接数≥200万
	8. 入侵检测系统（IDS）	满检速率≥15Gbps

		最大并发连接数≥500万
	9. 入侵防御系统（IPS）	满检速率≥20Gbps 最大并发连接数≥500万
	10. 安全隔离与信息交换产品 （网闸）	吞吐量≥1Gbps 系统延时≤5ms
	11. 反垃圾邮件产品	连接处理速率（连接/秒）>100 平均延迟时间<100ms
	12. 网络综合审计系统	抓包速度≥5Gbps 记录事件能力≥5万条/秒
	13. 网络脆弱性扫描产品	最大并行扫描IP数量≥60个
	14. 安全数据库系统	TPC-E tpsE（每秒可交易数量）≥ 4500个
	15 网站恢复产品（硬件）	恢复时间≤2ms 站点的最长路径≥10级

附件 2

信息安全保障能力基本要求

保障类	保障组件
ADV：开发	ADV_ARC.1 安全架构描述
	ADV_FSP.2 安全执行功能规范
	ADV_TDS.1 基础设计
AGD：指导性文档	AGD_OPE.1 操作用户指南
	AGD_PRE.1 准备程序
ALC：生命周期支持	ALC_CMC.2 CM系统的使用
	ALC_CMS.2 部分TOE CM覆盖
	ALC_DEL.1 交付程序

附件 3

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, 生产企业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

生产企业应规定与质量活动有关的各类人员职责及相互关系, 且生产企业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

生产企业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) 生产企业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) 生产企业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) 生产企业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) 生产企业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) 生产企业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) 生产企业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。