编号：CCRC-CCIS-2023

网络关键设备和网络安全专用产品安全认证实施细则

2023-11-15 发布　　2023-11-21 实施

中国网络安全审查技术与认证中心 发布

目 录

1.适用范围

本细则依据《网络关键设备和网络安全专用产品安全认证实施规则》制定，规定了网络关键设备和网络安全专用产品安全认证的实施程序。

2.认证依据标准

网络关键设备认证依据的标准为GB 40050，网络安全专用产品认证依据的标准为GB 42250。

3.认证模式

型式试验 + 获证后监督

4.认证单元划分

认证机构按产品型号/版本/企业分级划分认证单元。同一认证单元内有多个型号/版本的产品时，需要认证委托人提交型号/版本间的差异说明，必要时还应对差异部分补充检测。

5.认证实施程序

5.1 认证委托

认证委托人向认证机构递交认证委托，并按要求提交文件。认证委托文件包括：

1）基本信息：

- 认证申请书；
- 营业执照、事业单位法人证书或具有同等效力的法律地位证明材料。

2）产品技术文件：

- 产品功能说明书和/或使用手册；
- 安全保障能力文件；
- 同一认证单元中型号/版本间的差异说明（如适用）。

3）安全质量持续符合能力自查报告

认证机构对委托文件进行审核，确定认证委托人提交文件满足要求后，受理该委托。

5.2 型式试验

5.2.1 型式试验样品

5.2.1.1 送样要求

型式试验的样品由认证委托人按型式试验方案选送代表性样品，每种产品送样 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指定的实验室，递送时应采用防护措施，防止样品损坏。

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。

5.2.1.2 样品的处置

认证结束后，实验室向认证委托人返回型式试验样品或受认证委托人授权处置样品。

5.2.2 型式试验的实施

实验室按照认证依据标准，并参考与之相配套的、针对具体

产品类别的国家标准实施检测（不含安全保障要求部分）。

对型式试验发现的不符合项，允许整改，并由实验室对相关项目重新检测。

对型式试验全过程做出完整记录，并妥善管理、保存、保密相关文件，确保检测结果可追溯。

5.2.3 型式试验报告的提交

认证机构制定统一的型式试验报告格式。

型式试验结束后，实验室应根据认证机构的要求及时向认证机构和认证委托人出具型式试验报告。认证委托人应妥善保管型式试验报告，确保获证后监督时能够向认证机构提供。

5.2.4 安全保障能力评估

由认证机构指派评价人员按照认证依据标准，并参考与之相配套的、针对具体产品类别的国家标准实施安全保障能力评估。评估的方式为文件评估。

对评估过程中发现的不符合项，允许整改。

评估全过程应完整记录，并妥善管理、保存、保密相关文件，确保评估结果可追溯。

认证机构制定统一的评估技术报告格式。

评估结束后，评估人员向认证机构提交评估技术报告，并向认证委托人出具评估技术报告。认证委托人应妥善保管评估技术报告，确保获证后监督时能够向认证机构提供。

5.2.5 型式试验时限

各类产品型式试验时限参照下表。

序号	设备/产品类别	型式试验时限 （单位：工作日）
1	路由器	28
2	交换机	28
3	服务器（机架式）	28
4	可编程逻辑控制器（PLC 设备）	28
5	数据备份与恢复产品	28
6	防火墙	28
7	入侵检测系统（IDS）	28
8	入侵防御系统（IPS）	28
9	网络和终端隔离产品	28
10	反垃圾邮件产品	28
11	网络安全审计产品	28
12	网络脆弱性扫描产品	28
13	安全数据库系统	55
14	网站数据恢复产品	28
15	虚拟专用网产品	20
16	防病毒网关	28
17	统一威胁管理产品（UTM）	28
18	病毒防治产品	28

序号	设备/产品类别	型式试验时限 （单位：工作日）
19	安全操作系统	55
20	安全网络存储	28
21	公钥基础设施	28
22	网络安全态势感知产品	28
23	信息系统安全管理平台	28
24	网络型流量控制产品	20
25	负载均衡产品	20
26	信息过滤产品	20
27	抗拒绝服务攻击产品	20
28	终端接入控制产品	20
29	USB 移动存储介质管理系统	20
30	文件加密产品	20
31	数据泄露防护产品	20
32	数据销毁软件产品	20
33	安全配置检查产品	20
34	运维安全管理产品	20
35	日志分析产品	20
36	身份鉴别产品	20
37	终端安全监测产品	20
38	电子文档安全管理产品	20

上述时间不含因产品不合格，进行整改和复试的时间。

5.3 认证结果评价与批准

认证机构对型式试验及相关文件信息等进行综合评价，做出认证决定。对于符合认证要求的，颁发认证证书（每一个认证单元颁发一张认证证书）并允许使用认证标志。对于不符合认证要求的，向认证委托人发送认证不通过通知书。

5.4 获证后监督

5.4.1 企业分级管理

认证机构根据诚信守法状况、所生产产品质量状况等与质量相关的信息进行综合评价，将生产者分为高、中、基本三级。分级原则详见附件 1。

5.4.2 监督的实施方式

获证后监督的实施方式包括：

1）安全质量持续符合能力评价

安全质量持续符合能力评价（简称能力评价）内容详见《安全质量持续符合能力要求》（本细则附件 2）。

能力评价的实施方式为生产者、生产企业现场检查，人日数根据产品类别确定。现场检查 2 人日起，每增加一类产品增加 0.5 人日。当涉及多场所时，每增加一个场所增加 1 人日。

对发现的不符合项，允许整改，并经认证机构确认整改结果。

2）产品抽样检测

产品抽样检测的实施方式为从生产现场抽取样品，由指定实验室进行检测。认证机构制定抽样方案，并提前 3 个月通知生产者。生产者应配合认证机构在规定的时限内完成抽样，并将样品送至指定实验室。由认证机构确定检测内容。实验室在 20 工作日内完成检测工作。

3）自检自查

认证委托人组织生产者、生产企业由经认证机构授权的具备能力的人员依据《安全质量持续符合能力要求》进行自查，依据标准对获证产品进行自检，并向认证机构提交自查报告和自检报告。认证机构制定统一的自查报告和自检报告模板。

5.4.3 监督的实施

监督每 5 年为一个周期。每年的监督安排如下表所列：

企业分级	第一年	第二年	第三年	第四年	第五年
高	能力评价	自检自查	自检自查	产品检测	自检自查
中	能力评价	自检自查	产品检测	自检自查	产品检测
基本	能力评价	产品检测	自检自查	产品检测	产品检测

5.4.4 特殊监督的实施

如果发生下述情况之一，可安排特殊监督：

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）有足够信息表明生产者、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。

当发生以上 1)、2）情形时，特殊监督以产品检测的方式实施，当发生以上 3）情形时，特殊监督以能力评价的方式实施。实施要求参见 5.4.2。

5.4.5 获证后监督结果的评价

认证机构对获证后监督结论和相关文件信息进行综合评价。评价通过的，可继续保持认证证书、使用认证标志；评价不通过的，认证机构应当根据相应情形作出暂停或者撤销认证证书的处理，并予以公布。

5.5 认证时限

型式试验时限依据本细则 5.2.5 要求。受理、认证结果评价与批准、证书制作等其他环节认证工作合计一般不超过 3 工作日。

6.认证证书

6.1 认证证书的保持

认证证书有效期为 5 年。在有效期内，通过认证机构的获证后监督，保持认证证书的有效性。认证证书有效期届满，需要延续使用的，认证委托人应在有效期届满前 90 天内提出认证委托。认证有效期内最后一次获证后监督结果合格的，认证机构换发新证书。

6.2 认证证书的变更

若获证产品或其生产者、生产企业等发生变化，或认证要求发生变更时，认证委托人应向认证机构提出变更委托。

认证机构根据变更的内容，对委托文件进行评价，确定是否可以批准变更。如需进行检测和/或安全质量持续符合能力评价，应在检测和/或评价合格后，方可批准变更。

6.3 认证证书覆盖产品的扩展

认证委托人需要扩展已经获得的认证证书覆盖的产品范围时，应向认证机构提出扩展委托，并提供扩展产品和获证产品之间的差异说明。

认证机构根据扩展的内容，对委托文件进行评价，确认原认证结果对扩展产品的有效性，必要时，对差异部分补充检测。认证机构根据委托文件、检测情况进行综合评价，做出认证决定。对符合认证要求的，换发认证证书。

6.4 认证证书的暂停、注销和撤销

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》和认证机构的有关规定执行。在认证证书暂停期间及认证证书注销和撤销后，获证机构不得继续使用证书。

7.认证标志

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，不允许变形。

7.3 加施方式

可以采用统一印制的标准规格标志，或模压、铭牌印刷、软件加施等方式。

7.4 标志位置

硬件产品应当在本体的铭牌附近加施认证标志。

软件产品应当在其软件包装/载体上加施认证标志，如该软件产品不使用包装/载体，则应当在软件使用的许可协议中的显著位置明确该产品已经获得认证。

8.认证责任

认证机构应当对其做出的认证结论负责。

实验室应当对其检测结果和检测报告负责。

认证委托人应当对其所提交的认证委托文件及样品的真实性、合法性负责。

附件 1

企业分级原则

一、综述

依据《网络关键设备和网络安全专用产品安全认证实施规则》，认证机构根据诚信守法状况、所生产产品质量状况等与质量相关的信息进行综合评价，对生产者进行分级。本细则将生产者分为“高”、“中”、“基本”三级。

二、分级原则

认证机构根据认证评价情况、企业提供资料、外部质量信息等对生产者进行综合评价，确定并动态调整企业分级。

（一）信息的获取

认证机构通过以下渠道获取企业分级所需的信息：

1. 认证评价

包括检测情况、安全质量持续符合能力评价情况等。

2. 收集外部质量信息

包括产品质量监督抽查、申投诉、主管部门发布的相关公告等。

3. 企业申报材料

生产者可随时向认证机构报送综合评价所需信息和证明文

件。

（二）综合评价

认证机构对以下内容进行综合评价并打分：

（1）获得相关权威认证机构颁发的体系、产品等认证证书。

（2）获得国家级、省级相关领域科技奖项，或荣誉称号等。

（3）近两年获证后监督，安全质量持续符合能力评价、产品检测结果。

（4）近三年是否发生违反认证证书及认证标志使用规定的情况。

（5）近三年获证同类产品在国家、地方、行业等产品质量监督抽查中结果。

（6）近三年是否发生获证同类产品引发的安全事故。是否发生经证实的重大投诉。

（7）近三年是否发生违法违规的情况，认证过程中是否发生样品、文件造假等不诚信的情况。

认证机构按以下公式对评价情况计算综合得分：

$$T=\sum_{i=1}^{n}S_iW_i$$

T：综合得分

n：评价项目总数

S：单项得分

W：单项权重

（三）企业分级

认证机构根据综合评价及评分情况，按以下条件确定企业分级。

高：T≥90

中：80≤T<90

基本：T<80

附件 2

安全质量持续符合能力要求

为保证批量生产的认证产品与型式试验样品的一致性，生产者/生产企业应满足本文件规定的安全质量持续符合能力基本要求。

一、能力要求

对生产者/生产企业在安全质量持续能力方面提出以下要求。

1. 认证产品一致性

a）应对所生产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标准的要求。

b）应对产品进行配置管理，建立并维护配置项列表。

c）当认证产品发生变更时，应向认证机构申报，由认证机构确认产品符合认证要求后方可使用认证证书和认证标志。

d）在产品出厂前，应对产品运行正确性进行确认，并对产品配置情况进行一致性检查。

2. 测试

a）在产品的软件（包括固件）发布前，应进行测试。测试的内容应覆盖并达到相应产品国家标准中安全功能及自身安全要求。

b）应具备测试人员，测试人员应熟悉产品标准，并具备相应测试能力。生产企业应具备测试所需的各类仪器设备（含软件工具），并对其进行维护和管理。

c）委托外部机构实施测试的，应对机构能力进行确认，并纳入供应链管理。

3. 脆弱性评定

a）应对产品进行脆弱性评估，以确保产品不包含已公开的中、高风险漏洞。

b）应建立和执行针对产品安全缺陷、漏洞的应急响应机制和流程，对发现的产品安全缺陷和漏洞采取修复或替代方案等补救措施，及时告知用户安全风险和可用的补救措施。当缺陷和漏洞可能造成产品不符合认证要求时，应向认证机构报告。

4. 供应链安全

a）应识别产品关键部件，对供应商进行选择、评价和日常管理。

b）应具备供应链各环节核心要素追溯能力。

c）应对供应链安全进行风险防控，收集质量、安全等相关信息，识别可能发生的供应链安全事件。当发生可能影响产品的标准符合性的事件时，应及时采取补救措施，并向认证机构报告。

二、评价要求

安全质量持续符合能力评价的基本内容包括标准符合性检

查和安全质量持续符合能力检查。

（一）标准符合性检查

认证机构按认证的产品类别在生产企业现场抽取样品，根据认证依据标准选定项目，在生产企业人员配合下对产品与认证标准的符合性进行检查。

检查的项目从 GB 40050、GB 42250 及与之相配套的、针对具体产品类别的国家标准中选取。

（二）安全质量持续符合能力检查

1. 产品一致性检查

认证机构在生产企业现场，按认证的产品类别抽取样品进行一致性检查。

a）查认证产品的生产者（制造商）、生产企业的信息是否与认证证书内容一致；

b）查认证产品及铭牌上标识的产品名称、型号规格、认证标志等信息，与型式试验报告是否一致；

c）查认证产品软件、硬件、固件等是否与型式试验报告、认证机构批准的产品变更信息一致；

d）查产品配置管理情况，应具备配置项列表，配置项的发布应经过确认和审批。

e）查出厂前对产品的确认和检查情况，应能够确保产品启动、运行的正确性及产品一致性。

f）抽取部分安全功能和自身安全要求项目验证认证产品与型式试验报告的一致性。

2. 测试

a）查产品的软件（固件）在发布前的测试过程证明文件，如测试记录、报告等，测试的内容应覆盖并达到相应产品国家标准中安全功能及自身安全要求。测试结论应能够证明该产品软件（固件）符合标准要求。

b）对测试人员进行能力评价，评价的内容包括人员是否熟悉产品标准，能否正确使用测试工具进行测试，记录过程并形成结论。查测试仪器设备（含软件工具），应能够满足产品标准中对安全功能、自身安全等要求的测试活动。查设备的维护和管理记录，应能够确保设备状态符合测试工作的要求。

c）如委托外部机构实施测试，查机构能力确认证明文件，应能够证明该机构具备依据国家标准对相应产品进行测试的能力。该机构出具的报告等文件应满足 a)的要求。供应链安全的检查内容中应包含对外部测试机构的管理。

2. 脆弱性评定

a）查脆弱性评定活动，应具备适宜的漏洞检查方法和手段。如使用漏洞检查工具，应确保漏洞库处于最新版本。如采用人工分析的方式，应确保相应人员具备脆弱性评定能力。

b）查生产企业对认证产品的安全缺陷、漏洞处置情况，应

能够及时采取修复或替代方案等补救措施。对已交付的产品，应采取适当的方式及时告知用户安全风险及可用的补救措施，如：发出邮件，发布通知、公告、补丁包等。当涉及已公开的中、高风险漏洞时，应及时向认证机构报告。

3. 供应链安全

a）查认证产品各组成部件（含软件、固件、硬件等）外部供应的情况，包括外包开发、外购等。当部件与产品的标准符合性相关时，应定义为关键部件。若关键部件由外部供应，查供应商的选择、评价和日常管理记录，应能确保供应商提供的部件可满足产品的安全及质量要求。

b） 供应链核心要素应至少包括产品研发、生产、测试等环节涉及的源代码、设计图、工具、产品部件等等。查供应链各核心要素的管理情况，各要素应能追溯到其来源并记录相关信息。应能够收集供应链各核心要素来源的产品质量、安全、信用等信息和变更情况，识别各类风险。当发生供应链安全事件时，应能够及时响应，避免出现产品安全质量问题。如安全事件可能影响到产品标准符合性时，应立即采取补救措施，并向认证机构报告。补救措施应覆盖已交付的产品。