编号：CCRC-IR-040:2026

IT 产品信息安全认证实施规则
云计算安全防护产品

2026-03-30发布　　2026-05-01实施

中国网络安全审查认证和市场监管大数据中心发布

目 录

1．适用范围

本规则适用于中国网络安全审查认证和市场监管大数据中心（CCRC）针对云计算安全防护产品开展的信息安全认证。

云计算安全防护产品是以软件版本方式或以互联网方式交付的，为云平台或其他云计算环境下的系统提供包括但不限于抗拒绝服务攻击、Web应用安全防护、内容过滤、虚拟防火墙、 网络脆弱性检测、主机安全防护、网络入侵检测等一种或多种安全防护组件的产品，并同时能够实现安全防护组件的自动化部署、授权自动分发、集中管控、日志统一收集等功能。

以软件版本方式交付的产品是指云计算开发商向其客户交付一个具体的软件版本，传统的软件产品交付模式大多是这种方式。此情况在私有云场景下比较典型。

以互联网方式交付的产品是指在互联网上部署，快速迭代的方式开发和发布，此情况在公有云场景下比较典型。

2．认证模式

型式试验 + 初始工厂检查 + 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初始工厂检查

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

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

云计算安全防护产品原则上按照产品及其安全防护组件的名称、型号和版本划分认证单元。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。

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：

● 中文产品功能说明书（含安全防护组件说明）；

● 中文产品使用手册；

●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）；

3) 安全保障要求方面的文档：

●生命周期支持；

●安全目标；

●开发文档；

●指导性文档；

●测试文档；

●脆弱性评定文档。

4.2.3 受理评审

认证机构对认证委托人提交的申请信息进行评审，确认申请信息的完整性和正确性。对于信息中存在的问题，返回认证委托人补充完善。认证机构应在两个工作日内处理申请，并向认证委托人反馈处理结果。认证对象列入国家信用信息严重失信主体相关名录时，不予受理。

4.3文档审核

对申请方提交的安全保障要求文档，认证机构应按照依据标准中的安全保障能力要求对文档进行审核。

4.4型式试验委托及实施

4.4.1检测机构资质要求

1）基本条件和技术能力能够持续符合资质认定与中国合格评定国家认可委员会（CNAS）认可的条件和要求，并确保管理体系有效运行。

2）具备能够公正、独立和有效的从事检测活动的技术与管理能力，确保依据相关标准或者技术规范规定的程序和要求，出具检验检测数据、结果。

4.4.2型式试验送样

4.4.2.1送样原则

以软件版本交付的产品，由申请方将样品送到检测实验室。

以互联网方式交付的产品，需由申请方配合检测实验室在对应云计算环境下完成检测环境和资源搭建。

如果测试环境有特殊要求，申请方需要提供相应的说明及辅助设备。

4.4.2.2送样要求和数量

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。

4.4.2.3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《网络安全技术 信息技术安全评估准则》
- CCRC-TR-089《云计算安全防护产品安全技术要求与测试评价方法》

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认证结果评价与批准

认证机构负责对型式试验结果、申请材料等进行综合评价，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张云计算安全防护产品信息安全认证证书，证书内容中体现相关安全防护组件的信息。

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。

4.6获证后监督

4.6.1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。

4.6.2监督的内容

获证后监督采用工厂检查的方式进行，针对信息安全保障能力、产品一致性和质量保证能力进行检查。

当以下情况发生时，认证委托人需提交样品到实验室重新进行检测：

1）现场一致性核查存疑，无法现场确认。包括但不限于铭牌/型号/版本号、软硬件配置、标识标注与型式试验报告不一致或疑似不一致，现场目视、核对、验证无法判定时。

2）认证关键要素变更未申报，如产品核心硬件、关键软件、信息安全关键组件、结构/参数发生变更，企业未按规则履行变更申请；

3）产品被市场监管抽检不合格、收到投诉举报 、质量舆情、行业发布风险预警等情况。

当发生1）、2）种情况，企业需要提交产品变更差异说明，针对变更内容进行检测；当发生3）种情况时，需要进行全项检测。

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。

4.6.3 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。

6.1.2 证书内容

证书应体现以下内容:

- 委托人名称、地址
- 产品名称、型号/版本
- 制造商名称、地址
- 生产厂名称、地址
- 认证依据的标准、技术要求
- 认证模式
- 证书编号
- 发证机构、发证日期、有效期
- 其他需要说明的内容2

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。

本规则覆盖的产品认证证书，如果其产品发生以下变更时，应向本中心提出变更申请:

1）认证产品的商标，持证人、制造商或生产厂（名称和/或地址、质量保障体系等）发生变化;

2）认证产品涵盖的安全防护组件发生变更时，应重新申请或变更申请。

3）其他影响认证结果的因素变更。

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，并提交扩展系列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

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:

信息安全保障能力评估项目

1. 生命周期支持

1.1配置管理能力

开发者的配置管理能力应满足以下要求:

a) 为云计算安全防御产品的不同版本提供唯一的标识;

b) 使用配置管理系统对组成云计算安全防御产品的所有配置项进行维护，并唯一标识配置项;

c) 提供配置管理文档，配置管理文档描述用于唯一标识配置项的方法。

1.2配置管理范围

开发者应提供云计算安全防御产品配置项列表，并说明配置项的开发者。配置项列表至少包含云计算安全防御产品、安全保障要求的评估证据和云计算安全防御产品的组成部分。

1.3交付程序

开发者应使用一定的交付程序交付云计算安全防御产品，并将交付过程文档化。在给用户方交付云计算安全防御产品的各版本时，交付文档应描述为维护安全所必需的所有程序。

2.开发

2.1 安全架构描述

开发者应提供云计算安全防御产品安全功能的安全架构描述，安全架构描述应满足以下要求:

- 与产品设计文档中对安全功能实施抽象描述的级别一致;
- 描述与安全功能要求一致的云计算安全防御产品安全功能的安全域;
- 描述云计算安全防御产品安全功能初始化过程为何是安全的;

- 证实云计算安全防御产品安全功能能够防止被破坏；
- 证实云计算安全防御产品安全功能能够防止安全特性被旁路。

2.2 功能规范

开发者应提供完备的功能规范说明，功能规范说明应满足以下要求：

- 完全描述云计算安全防御产品的安全功能；
- 描述所有安全功能接口的目的与使用方法；
- 标识和描述每个安全功能接口相关的所有参数；
- 描述安全功能接口相关的安全功能实施行为；
- 描述由安全功能实施行为处理而引起的直接错误消息；

证实安全功能要求到安全功能接口的追溯。

2.3 产品设计

开发者应提供产品设计文档，产品设计文档应满足以下要求：

- 根据子系统描述云计算安全防御产品结构；
- 标识和描述云计算安全防御产品安全功能的所有子系统；
- 描述安全功能所有子系统间的相互作用；
- 提供的映射关系能够证实设计中描述的所有行为能够映射到调用它的安全功能接口。

3.指导性文档

3.1 操作用户指南

开发者应提供明确和合理的操作用户指南，操作用户指南与为评估而提供的其他所有文档保持一致，对每一种用户角色的描述应满足以下要求：

- 描述在安全处理环境中被控制的用户可访问的功能和特权，包含适当的警示信息；
- 描述如何以安全的方式使用云计算安全防御产品提供的可用接口；
- 描述可用功能和接口，尤其是受用户控制的所有安全参数，适当时指明安全值；

- 明确说明与需要执行的用户可访问功能有关的每一种安全相关事件，包括改变安全功能所控制实体的安全特性；
- 标识云计算安全防御产品运行的所有可能状态（包括操作导致的失败或者操作性错误），以及它们与维持安全运行之间的因果关系和联系；
- 充分实现安全目的所必须执行的安全策略。

3.2准备程序

开发者应提供云计算安全防御产品及其准备程序，准备程序描述应满足以下要求：

- 描述与开发者交付程序相一致的安全接收所交付云计算安全防御产品必需的所有步骤；
- 描述安全安装云计算安全防御产品及其运行环境必需的所有步骤。

4.测试

4.1 覆盖分析

- 开发者应提供测试覆盖文档，测试覆盖描述应表明测试文档中所标识的测试与功能规范中所描述的云计算安全防御产品的安全功能间的对应性。

4.2 测试：安全执行模块

- 开发者应提供测试深度分析。

4.3 功能测试

开发者应测试云计算安全防御产品安全功能，将结果文档化并提供测试文档。测试文档应包括以下内容：

- 测试计划，标识要执行的测试，并描述执行每个测试的方案，这些方案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，表明测试成功后的预期输出；
- 实际测试结果和预期的测试结果一致。

4.4 独立性测试

- 开发者应提供用于测试的TOE。
- TOE应适合测试。
- 开发者应提供一组与开发者TSF功能测试中同等的一系列资源。

5.脆弱性评定

- 基于已标识的潜在脆弱性，云计算安全防御产品能够抵抗具有基本攻击潜力攻击者的攻击。