

编号：TRIMPS-ZY04-042：2024

网络安全产品认证实施规则
网络蜜罐系统

TRIMPS

2024-07-15 发布

2024-07-20 实施

公安部第三研究所

目 录

前 言	II
1 适用范围	1
2 认证依据	1
3 认证模式	1
4 认证相关术语和定义	1
5 认证实施	2
5.1 认证的基本环节	2
5.2 认证流程	2
5.3 认证申请及受理	3
5.4 文件评审	3
5.5 型式试验委托及实施	3
5.7 认证时限	6
6 获证后监督	6
6.1 监督的时机	6
6.2 监督的内容	6
6.3 监督的频次	7
6.4 获证后监督结果的评价	7
7 认证证书的管理	7
7.1 证书的有效性	7
7.2 认证证书的变更	8
7.3 认证证书覆盖产品的扩展	9
7.4 认证证书的暂停、注销和撤销	9
8 认证标志的使用	9
8.1 认证标志的样式	9
8.2 认证标志的使用	10
8.3 加施方式和位置	10
8.4 标志的可追溯	10
9 收费依据与要求	10
10 投诉、申诉及技术争议的流程及时限要求	11
附件 A	12
附件 B	13
附件 C	14
附件 D	17

前 言

本文件由公安部第三研究所组织起草和发布，版权归公安部第三研究所所有，任何组织及个人未经公安部第三研究所许可，不得以任何形式全部或部分使用。

起草单位：公安部第三研究所

主要起草人：俞优、杨元原、李海鹏、张艳、沈亮、宋好好、吴改云、张笑笑、徐君、施帅。

TRIMPS

1 适用范围

本文件依据《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，规定了开展网络安全产品—网络蜜罐系统认证的基本原则和要求。

网络蜜罐系统是由若干个能诱捕和收集攻击行为数据的蜜罐构建的网络体系架构，能够伪装成正常的业务系统，采用主动防御技术，迷惑攻击者、捕捉攻击者的行为信息并且能对攻击进行溯源。

2 认证依据

TRIMPS-JSGF-030:2024 《信息安全技术 网络蜜罐系统认证技术规范》。

JCTJ 005—2016 《信息安全技术 通用渗透测试检测条件》。

上述标准及规范文件以有效版本为准。认证委托人应通过查询认证相关网站等方式主动获取相关标准变化信息和认证检测标准的执行要求。

认证机构负责跟踪产品认证依据引用标准及技术规范的制修订等变化情况，并依据开展产品认证的有关规定，组织制定标准及技术规范制修订等变化的转换期及认证实施方案，并对外公布。认证机构应向认证委托人提供详细、准确的关于标准及规范变化情况的信息。

3 认证模式

文件评审+型式试验+获证后监督

4 认证相关术语和定义

4.1

生产者

设计、生产产品或委托他人设计、生产产品并以其名义/商标进行销售，应对产品质量负主体责任并具有独立法人资格的企业。

注 1：生产者需要确保产品符合相关的质量标准和认证要求。

4.2

生产企业

受生产者委托实际完成产品生产、装配的企业。

注 1：生产企业是产品生产的物理场所，它可能是生产者的一部分，也可能是独立于生产者的外部加工单位。

注 2：在产品认证的过程中，生产企业需要确保其生产过程符合认证机构设定的标准和要求，以保证产品的质量和安全性。

5 认证实施

5.1 认证的基本环节

认证的基本环节包括：认证申请及受理、文件评审、型式试验委托及实施、认证结果评价与批准、获证后监督等。

5.2 认证流程

认证委托人向认证机构提交申请认证，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，确认合格后向认证机构指定的检测机构安排检测任务，并通知认证委托人根据本文件 5.5 的要求送样检测。检测机构依据本文件第 2 条规定的检测依据进行检测，并在完成检测后向认证机构提交检测报告。认证机构对型式试验、文件审核等内容进行综合评价，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。

5.3 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。

5.3.1 认证的单元划分

原则上，按产品型号/版本申请认证，若产品的关键件相同的可作为同一单元申请认证，产品关键件的要求按照本文件附件 A 的相关规定。

5.3.2 申请资料要求

认证委托人在申请网络蜜罐系统的网络安全认证时，需按照本文件附件 B 的要求提交认证资料。

5.4 文件评审

对认证委托人提交的符合本文件附件 B 要求的资料和文档，认证机构按照本文规定的认证依据进行审核。

5.5 型式试验委托及实施

5.5.1 送样时机及数量

认证委托人/生产企业可在文件审查通过后，按照认证机构规定要求将样品送到指定检测机构进行型式试验。样品数量一般每种产品为 2 套。

5.5.2 抽样方式及地点（适用于获证后监督）

认证机构指定人员在生产企业确认的合格品中随机抽取样品并封样（粘贴认证机构统一发放的封样条），样品数量一般每种产品为 2 套抽样 2 套，抽查基数原则上不低于 5 倍基数，如有特殊需求可增加样品数量。

认证委托人应确保型式试验样品在到达认证机构指定的检测机构前，封样条不被破坏，并负责将样品送至检测机构。

5.5.3 样品确认

指定检测机构收到样品后，对样品进行确认并将确认的信息通报认证机构。当发现样品未及时送达，或样品与送样要求信息不一致时，应及时通知认证机构。

5.5.4 型式试验依据及检测项目

型式试验依据标准规范及检测项目见附件 C。

5.5.5 型式试验实施

认证机构向指定检测机构下达型式试验委托检测任务。

指定检测机构应依据国家认监委相关规定和认证机构的相关要求，在规定时间内完成样品检测，确保检测结论真实、准确。

指定检测机构应建立、实施并保持样品型式试验检测过程控制的可追溯体系。型式试验过程发现异常情况时，应及时与认证机构沟通，并依据认证机构的指令做出相应处理。

型式试验结束后，指定检测机构应以适当的方式处置试验样品并归档保存相关记录和资料。

5.5.6 型式试验报告

型式试验结束后,指定检测机构应按认证机构规定的统一格式出具一式两份型式试验报告,并在规定的时限内送达认证机构。指定检测机构应确保试验报告的正确性和真实性。

检测机构及其相关人员应对其做出的型式试验报告内容及检测结论正确性负责,对检测结果保密。

认证机构将型式试验报告随认证决定一并发给认证委托人。

认证委托人应保存型式试验报告原件,在获证后监督时应能向认证机构和执法机构提供完整有效的型式试验报告。

5.5.7 型式试验不合格处置

当型式试验检测结果有不合格时,允许认证委托人/生产企业进行整改。认证委托人应在3个月内完成整改并向认证机构提交齐全的整改材料同时按照认证机构要求提交复试样品。当复试检测项目符合要求时,为型式试验通过;否则为不通过,终止认证。

整改应在规定期限内完成,超过规定期限未完成整改和/或未送达复试检测样品的,视为认证委托人放弃认证委托,终止认证;认证委托人也可主动终止委托。生产企业完成整改后,认证委托人可重新提出认证委托。

5.5.8 样品及相关资料的处置

认证结束后,认证委托人可向检测机构申请取回型式试验样品,相关申请资料由认证机构、检测机构妥善处置。

5.6 认证结果评价与批准

认证机构负责对型式试验、文件审查结果等进行综合评价，评价合格的，做出认证决定。对符合认证要求的，认证机构予以批准认证，颁发认证证书。对认证决定过程中发现不符合认证要求项，允许限期整改，整改期限一般不超过 3 个月，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。对整改后仍不符合认证要求的，认证机构不予批准认证委托，认证终止。

5.7 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 获证后监督

6.1 监督的时机

认证证书持有者向认证机构提出到期换证申请时，认证机构应对认证产品的全部项目进行监督复测。

监督复测应在认证证书到期前三个月内完成。证书到期后，获证后监督逾期未完成的，认证机构根据相应情形做出暂停、撤销、注销相关认证证书的决定，通知认证委托人并予公布。

6.2 监督的内容

通常情况下，按照本文件 5.5 和附件 C 的要求完成全部项目的监督复测，检测合格的重新换发认证证书，不合格的按照本文件 7.4 的要求对证

书做出处理。

必要时按照附件 D 的要求完成工厂检查，并按照本文件 5.5.2 要求完成抽样。

6.3 监督的频次

监督频次一般为两年一次，必要时，认证机构可调整监督频次，增加监督频次的情形包括但不限于下述情况之一：

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。

6.4 获证后监督结果的评价

获证后监督的结果综合评价包括监督抽样复测结果评价及工厂检查（必要时）结果评价。综合评价结果通过时，认证机构向认证委托人发出新的认证证书，准许继续使用认证证书和标志；评价结果不通过的，认证机构根据相应情形做出暂停、撤销相关认证证书的决定，通知认证委托人并予公布。

7 认证证书的管理

7.1 证书的有效性

本文件覆盖的产品认证证书有效期为 2 年。认证证书有效期届满，需要延续使用的，持证人应当在认证证有效期界满前 90 天内申请监督复测。

7.2 认证证书的变更

7.2.1 变更的申请

获证后的产品，如果认证证书如发生如下变化时，认证证书持有者应向认证机构提出正式变更申请。

1) 证书中的认证委托人、生产者、生产企业名称和/或地址变更(不含搬迁)，经资料评审后，可直接换发认证证书，原证书收回；

2) 当生产企业(场所)地址变更(实际搬迁)时，认证机构经评估需进行产品检测的，证委托人应按照认证机构评估确定的送样检测方案实施送样检测。当认证机构评估符合要求时，换发认证证书，原证书收回；

3) 产品标准、技术规范和/或实施规则变更时，认证机构发布转换公告并实施转换。转换符合要求的换发证书，原证书收回。逾期未完成转换的，暂停原认证证书；

4) 当对标准符合性或产品一致性发生影响的控制点(即涉及附件 A 规定的《网络蜜罐系统 网络安全认证关键控制点》)变化时，应重新申请认证。

7.2.2 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。

7.2.3 证书的有效期

证书在进行变更后，其有效期按照变更类别的不同重新给定。

7.3 认证证书覆盖产品的扩展

7.3.1 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。

7.3.2 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。

7.3.3 证书的有效期

证书在进行扩展后，其有效期与原证书一致。

7.4 认证证书的暂停、注销和撤销

按照 TRIMPS-MR-7.11-02 《关于认证证书暂停、恢复、注销、撤销的通告》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。

8 认证标志的使用

8.1 认证标志的样式



8.2 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。

8.3 加施方式和位置

证书持有者应按认证机构关于认证标志管理的相关规定使用认证标志。硬件产品可以在产品本体、铭牌或包装上加施认证标志。

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。

8.4 标志的可追溯

证书持有者应对认证标志的加施情况完整记录，使认证标志的使用可追溯。

9 收费依据与要求

认证收费由认证机构依据国家及机构的有关规定收取。

原则上，初次委托企业的相关认证费用应在认证委托时交纳，获证后

监督费用应在监督检查实施时交纳。

对于未能交纳相关认证费用的，认证机构做出终止认证、暂停证书及撤销证书的决定。

10 投诉、申诉及技术争议的流程及时限要求

按照认证机构相关的投诉、申诉及技术争议处理程序要求进行。

TRIMPS

附件 A

网络蜜罐系统 网络安全认证关键控制点

A.1 功能关键控制点

产品级别	认证一致性关键控制点
基本级	1、软件版本、支撑操作系统类型 2、伪装欺骗、攻击诱导、攻击事件记录、攻击事件分析、攻击事件告警、安全控制、标识与鉴别、安全管理、安全审计
增强级	1、软件版本、支撑操作系统类型 2、伪装欺骗、攻击诱导、攻击事件记录、攻击事件分析、攻击事件告警、安全控制、联动防护、标识与鉴别、安全管理、安全审计

A.2 硬件关键件

网络蜜罐系统的硬件关键件应至少包括：处理器、内存、存储设备、网络接口。

附件 B

认证委托时需提交的资料

- 1) 申请基本信息：
 - a. 认证申请书；
 - b. 认证委托人声明；
 - c. 相关法律地位证明材料（复印件）；
 - e. 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
- 3) 产品相关说明：
 - a. 中文产品功能说明书和/或使用手册；
 - b. 中文铭牌和警告标记；
 - c. 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）；
 - d. 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：

认证依据标准/规范中对应级别安全保障要求相应的文档。
- 5) 安全功能相关说明文件。
- 6) 认证机构要求的其他资料。

附件 C

网络蜜罐系统 认证依据标准规范及检测项目

C.1 认证依据 1：TRIMPS-JSGF-030：2024《信息安全技术 网络蜜罐系统 认证技术规范》

依据安全功能、自身安全功能、安全保障要求的广度和强度，将产品分为基本级、增强级两个等级，各等级产品对应的检验项目如下表所示。

检测项目		基本级	增强级	
安全功能 要求	伪装欺骗	欺骗环境支持	7.1.1 a)~b)	7.1.1
		蜜罐类型支持	7.1.2	7.1.2
		漏洞部署支持	—	7.1.3
	攻击诱导	欺骗诱饵	7.2.1	7.2.1
		诱捕节点	7.2.2	7.2.2
		转移攻击流量	7.2.3	7.2.3
		虚拟流量	—	7.2.4
	攻击事件记录	事件内容	7.3.1 a)~d)、f)	7.3.1
		事件类型	7.3.2 a)~f)	7.3.2
		事件过滤	7.3.3	7.3.3
	攻击事件分析	关联分析	7.4.1 a)~e)	7.4.1
		统计报表	—	7.4.2
		威胁情报	—	7.4.3
	攻击事件告警	告警设置	7.5.1	7.5.1
		告警等级	—	7.5.2
		告警策略	7.5.3	7.5.3
		告警方式	7.5.4	7.5.4
		告警白名单	7.5.5	7.5.5
	联动防护		—	7.6
	安全控制	欺骗环境部署管理	7.7.1	7.7.1
欺骗环境集中管理		7.7.2	7.7.2	
监控程序自保护		—	7.7.3	
管理端保护		—	7.7.4	

检测项目		基本级	增强级	
		攻击隔离	7.7.5	7.7.5
		攻击事件记录安全	7.7.6	7.7.6
		攻击事件记录备份	—	7.7.8
		恢复出厂设置	7.7.9	7.7.9
自身安全功能要求	标识与鉴别	用户标识	8.1.1	8.1.1
		身份鉴别	8.1.2 a)~c)	8.1.2
	安全管理	安全功能管理	8.2.1	8.2.1
		安全角色管理	8.2.2 a)	8.2.2
		远程保密传输	8.2.3	8.2.3
		可信管理主机	—	8.2.4
		数据完整性	—	8.2.5
		安全支撑系统	8.2.6	8.2.6
		系统时间同步	—	8.2.7
	安全审计	审计日志生成	8.3.1	8.3.1
		审计日志存储	8.3.2	8.3.2
		审计日志管理	8.3.3 a) ~b)	8.3.3
	安全保障要求	开发	安全架构	9.1.1
功能规范			9.1.2 a)~f)	9.1.2
实现表示			—	9.1.3
产品设计			9.1.4 a)~d)	9.1.4
指导性文档		操作用户指南	9.2.1	9.2.1
		准备程序	9.2.2	9.2.2
生命周期支持		配置管理能力	9.3.1 a)~c)	9.3.1
		配置管理范围	9.3.2 a)	9.3.2
		交付程序	9.3.3	9.3.3
		开发安全	—	9.3.4
		生命周期定义	—	9.3.5
		工具和技术	—	9.3.6
测试		覆盖	9.4.1 a)	9.4.1
		深度	—	9.4.2
		功能测试	9.4.3	9.4.3
		独立测试	9.4.4	9.4.4

检测项目		基本级	增强级
	脆弱性评定	9.5	9.5

注：“——”表示该级别不适用

C.2 认证依据 2:JCTJ 005—2016《信息安全技术 通用渗透测试检测条件》

根据委托产品的形态不同，需实施基本的渗透测试，如 6.2.1、6.2.2(若 B/S 方式管理)，其它检验项目可根据认证委托人要求实施。

检测项目		规范条款
信息收集		6.1
漏洞扫描	网络脆弱性扫描	6.2.1
	WEB 应用脆弱性扫描	6.2.2
	移动智能终端脆弱性扫描	6.2.3
	其他脆弱性扫描	6.2.4
渗透测试	物理攻击	6.3.1
	业务逻辑攻击	6.3.2
	中间件攻击	6.3.3
	数据库类攻击	6.3.4
	工控设备类攻击	6.3.5
	APP 类攻击	6.3.6
社会工程学		6.4
代码审计 (可选)		6.5
性能测试 (可选)		6.6

附件 D

工厂检查

D.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。

D.2 信息安全保障能力基本要求

详见认证依据标准/规范中对应级别安全保障要求。

D.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。

D.3.1 职责和资源

D.3.1.1 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。

D.3.1.2 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文件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。

D.3.1.3 认证产品一致性

1) 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；

2) 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。

D.3.1.4 认证产品外购部件或外包软件模块管理

1. 外购部件供应商或软件模块的外包商的控制

1) 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；

2) 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。

2. 外购部件或外包软件模块的验证

1) 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；

2) 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。

D.4 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。

D.5 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，并适当考虑生产者、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。