编号：TRIMPS-ZY04-004：2023

# 网络安全产品认证实施规则

## 互联网上网服务营业场所

## 信息安全管理系统产品



2023-06-13 发布　　2023-07-01 实施

公安部第三研究所

# 目 录

# 前　言

本实施规则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：顾建新、沈亮、宋好好、李海鹏、吴改云、徐君、施帅。

## 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，规定了开展网络安全类产品--互联网上网服务营业场所信息安全管理系统产品认证的基本原则和要求。

互联网上网服务营业场所是指以收费方式为公众提供互联网上网服务的场所（俗称“网吧”），互联网上网服务营业场所信息安全管理系统是指部署在互联网上网服务营业场所的信息安全管理系统。通过该系统的部署，不仅能为营业场所提供部分运维管理功能，更能为管理部门提供相关上网信息的审计服务。

## 2.认证模式

型式试验 + 获证后监督

## 3.认证依据标准

GA 557.1～557.12-2005《互联网上网服务营业场所 信息安全管理代码》、

GA 558.1～557.8-2005《互联网上网服务营业场所 信息安全管理系统数据交换格式》、

GA 559-2005《互联网上网服务营业场所信息安全管理系统营业场所端功能要求》、

GA 561-2005《互联网上网服务营业场所信息安全管理系统管理端功能要求》、

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。

## 4.认证实施

### 4.1 认证的基本环节

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

### 4.2 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规则 4.5 的要求送样检测。检测机构依据本规则第 3 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。

### 4.3 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。

#### 4.3.1 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规则附件 1 的相关规定。

对于多于一个型号/版本的产品作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。

#### 4.3.2 申请资料要求

认证委托人在申请互联网上网服务营业场所信息安全管理系统产品的网络安全认证时，需按照本规则附件 2 的要求提交认证资料。

### 4.4 文档审核

对认证委托人提交的符合本规则附件 2 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。

### 4.5 型式试验委托及实施

#### 4.5.1 型式试验抽样

##### 4.5.1.1 抽样要求

按照本规则认证单元划分的原则，对确定申请的认证单元进行送样。认证机构通过远程方式完成型式试验样品的随机选择，并在远程监控下完成封样，粘贴认证机构统一发放的封样条，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。

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。

一般每种产品抽样 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。

#### 4.5.1.2 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。

### 4.5.2 型式试验依据

按照本规则附件 3 的要求进行。

### 4.5.3 型式试验报告的提交

型式试验一般由认证机构指定的检测机构在 30 个工作日内完成，型式试验完成后，检测机构应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。

## 4.6 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。

## 4.7 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。

## 5 获证后监督

### 5.1 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。

### 5.2 监督的时机

监督复查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。

### 5.3 监督的内容

通常情况下，按照本规则 4.5 的要求完成全部项目的监督抽样复测，检测合格的重新换发认证证书 ,不合格的按照本规则 6.4 的要求对证书做出处理。

必要时按照附件 4 的要求完成工厂检查。

### 5.4 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。

## 6.认证证书的管理

## 6.1 证书的有效性

证书有效期 2 年。

## 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 1

规定的《互联网上网服务营业场所信息安全管理系统产品 网络安全认证关键控制点》)变化时，应重新申请认证。

### 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，其有效期按照变更类别的不同重新给定。

## 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，获证机构不得继续使用证书。

## 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。

### 7.4 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。

## 8 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。

## 9、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。

附件 1

# 互联网上网服务营业场所信息安全管理系统产品网络安全认证关键控制点

## 1.1 软件产品关键控制点

| 认证一致性关键控制点 |
| --- |
| 1. 支撑操作系统版本、软件版本 |
| 2. 营业场所辅助管理 |
| 3. 上网人员权益保护 |
| 4. 信息安全管理 |
| 5. 营业场所端运行安全保障 |
| 6. 营业场所端与管理端数据交换 |
| 7. 其他管理要求 |
| 8. 营业场所管理功能 |
| 9. 信息安全审计功能 |
| 10. 网络虚拟人口库管理 |
| 11. 信息处理功能 |
| 12. 系统安全 |



## 1.2 硬件产品关键件

互联网上网服务营业场所信息安全管理系统产品的硬件关键件应至少包括：处理器、内存、存储设备、主板、网络接口

附件 2

# 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~~b.相关法律地位证明材料（复印件）；

~~e~~c.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.认证标准的适用性说明；

c.产品研制主要技术人员情况表；

d.产品测试技术人员情况表；

e.产品测试使用的主要设备表；

f.中文铭牌（硬件产品）；

g.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）；

h.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：

a.开发

b.指导性文档

c.生命周期支持

d.测试

e.脆弱性评定

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 3

# 互联网上网服务营业场所信息安全管理系统产品

# 自愿性认证依据标准规范及检测项目

## 1、认证依据 1

| 检测项目 | | | 认证依据 |
|---|---|---|---|
| 营业场所端功能要求 | 营业场所辅助管理 | 营业场所出口 IP 地址管理 | GA 557.1～557.12-2005《互联网上网服务营业场所信息安全管理代码》、GA 558.1～557.8-2005《互联网上网服务营业场所 信息安全管理系统数据交换格式》、GA 559-2005《互联网上网服务营业场所信息安全管理系统营业场所端功能要求》、GA 561-2005《互联网上网服务营业场所信息安全管理系统管理端功能要求》 |
| | | 营业终端登录管理 | |
| | | 营业场所端上网卡管理 | |
| | | 营业场所端上网人员信息管理 | |
| | | 统计分析管理 | |
| | 上网人员权益保护 | | |
| | 信息安全管理 | 有害信息过滤 | |
| | | 上网日志管理 | |
| | 营业场所端运行安全保障 | 标识与鉴别 | |
| | | 系统操作日志 | |
| | | 安全服务 | |
| | 营业场所端与管理端数据交换 | 营业场所端上线数据和下线数据上传 | |
| | | 营业场所端运行状态信息上传 | |
| | | 上网日志上传 | |
| | | 信息安全审计策略的接收与生效 | |
| | | 审计结果信息上传 | |
| | | 消息管理 | |
| | | 数据交换安全性保障 | |
| | 其他管理要求 | | |
| 管理端功能要求 | 营业场所管理功能 | 营业场所信息的录入与维护 | |
| | | 营业场所处罚结果信息的维护 | |
| | | 对营业场所端发布消息 | |
| | | 营业场所运行状态管理 | |
| | | 营业场所营业状态管理 | |
| | 信息安全审计功能 | 在逃人员比对报警 | |
| | | 上网日志的接收 | |

| | | | |
|---|---|---|---|
| | | 审计策略的设置 | |
| | | 审计策略的生效 | |
| | | 审计策略的有效期 | |
| | | 审计策略库的更新 | |
| | | 审计结果信息的接收 | |
| | | 报警管理 | |
| | 网络虚拟人口库管理 | | |
| | 信息处理功能 | 营业场所信息查询 | |
| | | 网络虚拟人口库查询 | |
| | | 上网日志查询 | |
| | | 审计策略查询 | |
| | | 审计结果及报警事件查询 | |
| | | 消息查询 | |
| | | 系统操作日志查询 | |
| | | 统计功能 | |
| | | 显示和打印 | |
| | 系统安全 | 标识与鉴别 | |
| | | 用户和权限管理 | |
| | | 系统操作日志记录 | |
| | | 数据交互安全性保障 | |
| | | 其他要求 | |
| 产品安全性要求 | | | |

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 BS 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 4

# 工厂检查

## 4.1 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。

## 4.2 信息安全保障能力基本要求

| 保障类 | 保障组件 |
| --- | --- |
| 开发 | 安全架构 |
| | 功能规范 |
| | 产品设计 |
| 指导性文档 | 操作用户指南 |
| | 准备程序 |
| 生命周期支持 | 配置管理能力 |
| | 配置管理范围 |
| | 交付程序 |
| 测试 | 测试覆盖 |
| | 功能测试 |
| | 独立测试 |
| 脆弱性评定 | |

## 4.3 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。

4.3.1 职责和资源

4.3.1.1 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。

4.3.1.2 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。

4.3.1.3 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。

4.3.1.4 认证产品外购部件或外包软件模块管理

a．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。

b. 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。

4.4 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。

4.5 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。