



开放可信技术提供商标准（O-TTPS）1.2 版解析：技术演进、合规升级与全球供应链安全实践

作者：atsec 谢继来

关键词：O-TTPS 标准、ISO/IEC 20243、供应链安全、可信技术生态、可信合规认证、全生命周期管理、COTS ICT 安全、The Open Group

本文为 atsec 和作者技术共享类文章，旨在共同探讨信息安全的相关话题。转载请注明：atsec 和作者名称。

atsec(Beijing) information technology Co., Ltd
3/F, Block C, Bld.1, Boya C-Center, Life Science Park,
Changping District, Beijing, P.R. China, 102206
Tel +86 10 5305 6679
www.atsec.com

1. 引言: O-TTPS 的定义与核心价值

开放可信技术提供商标准 (O-TTPS: Open Trusted Technology Provider™ Standard) 是由 The Open Group 主导的国际性技术安全规范, 旨在通过可验证的供应链管理实践, 确保商用现货 (COTS: Commercial Off The Shelf) 信息和通信技术 (ICT: Information and Communication Technology) 的可信性与安全性。该标准通过预防恶意污染、假冒产品及供应链攻击, 服务于硬件/软件组件提供商、提供商、系统集成商、政府及企业采购方, 构建全球化的可信技术生态。其等效国际标准 ISO/IEC 20243 的同步更新, 进一步强化了其权威性与适用性。

atsec 作为 The Open Group 授权的安全评估机构, 为全球诸多的机构执行了基于 O-TTPS 标准的评估, 并持续贡献于产业以及被评估机构的供应链安全性的优化。

2. O-TTPS 的发展历程与全球协作框架

2.1 标准发展历程

- **2010 年:** The Open Group 成立开放可信技术论坛 (OTTF), 联合技术企业、政府及供应链利益相关方, 推动技术合作。
- **2013 年:** 发布首版 O-TTPS 标准, 确立供应链安全基线要求。
- **2015 年:** 经 ISO/IEC 批准, 正式成为国际标准 ISO/IEC 20243:2015。
- **2018 年:** 升级至 1.1.1 版 (对应 ISO/IEC 20243:2018), 优化漏洞管理与供应商评估流程。
- **2023 年:** 迭代至 1.2 版 (对应 ISO/IEC 20243:2023), 响应行业新兴威胁与技术实践。

2.2 标准核心目标与适用对象

- **核心目标:** 覆盖技术产品全生命周期 (设计、开发、交付、维护), 确保技术产品的完整性、可追溯性与抗风险能力。
- **适用对象:** 硬件/软件组件提供商、提供商、系统集成商、政府及企业采购方。

3. O-TTPS 1.2 版的技术演进与关键变更

3.1 强制性与推荐性条款重构

- **量化调整:** 强制要求从 55 项增至 69 项, 推荐项从 29 项缩减至 17 项, 强化了合规基线。
- **关键领域升级:**
 - **技术开发类:** 产品开发及安全工程方法的部分推荐要求变成了强制性要求。对于开发需求追踪, 配置管理, 漏洞管理, 补丁管理的要求有所加强。

- **供应链安全类**: 供应链安全方法的部分推荐要求变成了强制性要求。对于风险管理, 访问控制, 员工和承包商的管理, 安全传输, 销毁流程等要求有所加强。

3.2 新增技术要求

- **漏洞管理扩展**:
 - 新增最新发现的漏洞披露流程条款。
 - 要求建立持续的产品漏洞分析响应, 补丁研发及漏洞修复机制。
- **安全传输要求增强**:
 - 供应链的物理传输和数据传输需进行风险评估并持续改进。

4. 新旧版本认证过渡策略与实践指南

4.1 O-TTPS 标准 1.1.1 版认证的延续性

- **有效期**: 2025 年 8 月 1 日前, 现有 1.1.1 版本仍可用于首次认证及重新认证。
- **过渡窗口**: 2025 年 8 月 1 日后, 新提交的申请需采用 1.2 版进行认证, 再认证的机构在证书有效期即将到达前六个月需开始采用 1.2 版进行再认证, 但无立即升级的强制要求。

4.2 重新认证路径设计

- **主动升级**: 被认证机构可提前申请 1.2 版认证 (认证程序开放后 6 个月内需完成)。
- **被动过渡**: 在之前的认证周期结束时, 需符合最新生效版本或新版标准生效前 6 个月的版本。

4.3 兼容性声明与声誉保障

- 1.2 版不否定 1.1.1 认证的有效性, 两者在有效期内均被认可为可信合规证明。

5. 行业采纳与标杆实践

5.1 企业级应用案例 (根据 The Open Group 官网发布的认证信息及企业公开的信息)

- **希捷科技**: 通过 O-TTPS 认证优化硬盘供应链透明度, 实现固件来源追溯与防篡改验证。
- **IBM**: 将标准融入软硬件产品开发, 通过强制可追溯的配置管理降低第三方组件风险。

5.2 政府与采购方驱动

- **标准认证的实践举例**: **企业范围采购解决方案 (NASA SEWP: Solutions for Enterprise-Wide Procurement)** 和 **政府范围采购合同 (GWAC: Government-Wide Acquisition Contract)**: 接受供应商持有 O-TTPS 认证, 确保政府采购设备符合 ISO/IEC 20243 安全基线。
- **认证注册与查询**: The Open Group 维护完整的 [O-TTPS 认证注册记录](#), SEWP 的 ISO/IEC 20243 网页提供已经完成 O-TTPS 认证的合同所有者专项查询服务。

6. 结论：构建安全供应链的技术合规基石

O-TTPS 1.2 版确保 O-TTPS 标准已被纳入了 COTS ICT 提供商当前的最佳实践，以降低恶意污染和假冒产品的风险。这意味着根据 1.2 版进行认证的机构可以实施最先进的实践，在产业的竞争中保持供应链安全性的技术优势和领导力。

附录：资源与支持

- 认证咨询: info_cn@atsec.com
- 权威参考资料:
 - The Open Group O-TTPS 认证注册库
 - ISO/IEC 20243:2023 标准文本
 - NASA SEWP GWAC 合规指南
 - atsec 官网: www.atsec.com