# 采用 OTTPS 保护供应链安全

谢继来、刘岩，atsec 中国，2015 年 3 月

关键词：供应链安全、安全评估、OTTPS



开放可信技术供应商标准（O-TTPS）是一套用来解决商用现货（COTS）与信息通信技术（ICT）产品整个生命周期内软硬件完整性威胁的指南、要求以及建议。

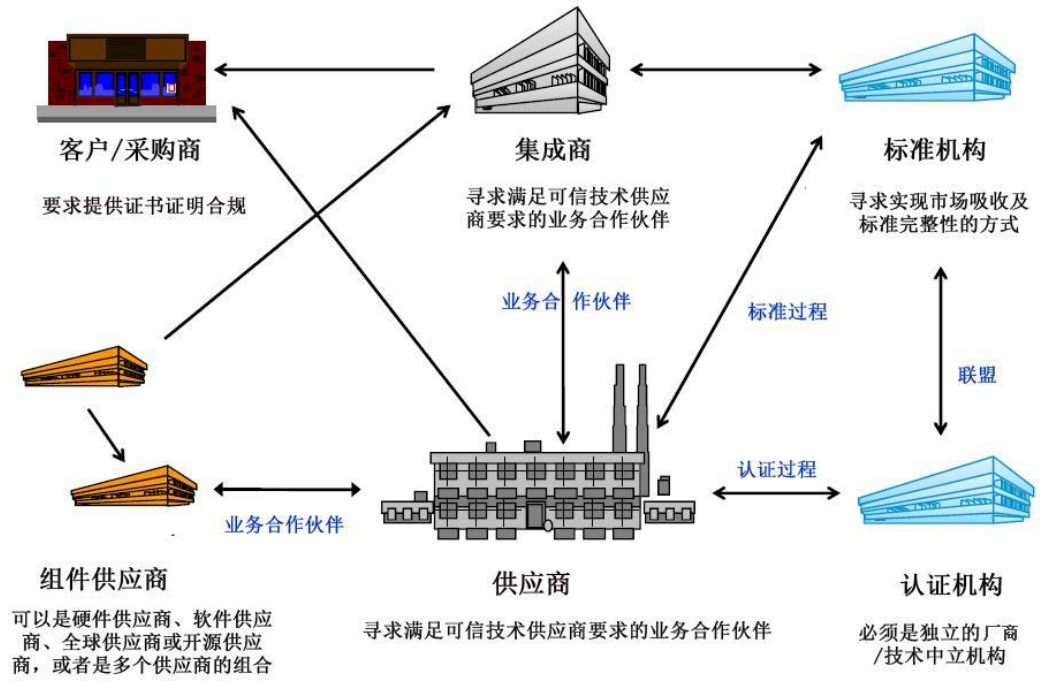
当今采购商在其 COTS ICT 采购中面临如下的两大威胁：

1. 受恶意污染的产品，即产品由供应商生产且经供应商授权的渠道购得，但产品已被恶意篡改。

2. 伪冒产品，即产品并非由供应商生产，或并非为供应商生产，或由未经供应商授权的渠道提供给供应商并被包装为合法正规产品（尽管其并不是合法正规产品）。

本标准的该初始版本用于解决与被恶意污染的产品及伪冒产品相关的威胁。

**经营场景示意图:**




经营场景相关方解释：

标准机构：开发某些认证标准及技术规范的组织。 本标准(OTTPS) 由国际开放标准组织可信技术论坛（The Open Group[1] Trusted Technology Forum）简称“OTTF[2]”

制定。

认证机构：提供认证与/或测试服务，尤其是参与合规性认证与/或测试的机构。 atsec[3] 是全球首批 OTTPS 认证体系的认可评估机构。atsec 从标准制定之初便积极参与了该标准的编写工作，且由 atsec 中国主导完成了该标准的中文版本的翻译和完善工作。

客户/采购商：从组件供应商、产品供应商或集成商处采购产品或服务。

集成商：为客户提供服务及解决方案。 这些服务及解决方案一般用于涉及多个供应商的大型项目。

供应商：构造产品，包括公司内部的产品或供应商提供的软件与/硬件组件。

组件供应商：组件供应商一般作为供应商的业务合作伙伴。

本标准要求供应商，组件供应商遵守 O-TTPS 标准要求及被认证为可信技术供应商，而客户/采购商及集成商则可以寻求可信技术供应商提供的产品或业务合作伙伴。

## OTTPS 合规的目标及效益

技术供应链日益向全球化、分割化及专业化方向发展。 所有商业及政府采购商、集成商、软件开发商、硬件供应商及生产商都是全球技术供应链的成员。 因此，全球社区的各个成员有责任确保端到端技术供应链的安全性。

OTTPS 合规可以使下列各方受益：

- **供应商：**采用这些实践的供应商能够在 COTS ICT 产品的开发、采购及维护流程中更好地识别及消减安全风险。 这些供应商能够利用与可信技术供应商身份相关的市场区分点，更轻易地从自己的供应商及商业合作关系中识别可信技术供应商。

- **组件供应商：**遵循最佳实践要求及建议的供应商还可获得可信技术供应商身份，能够充分利用与该身份相关的市场区分点，便于可信技术供应商及集成商之间结成更加密切、更加频繁的商业合作关系。

- **集成商：**集成商可从可信技术供应商及组件供应商处购买产品及组件（包括软件及硬件），促使基于外包及合作伙伴关系的集成工作变得更加安全、可信。 除此之外，遵守 O-TTPS 及作为可信技术供应商的集成商可以获得与上述供应商相同的利益。

- **采购商：**采购商可将供应商遵守 O-TTPS 作为其综合商业技术采购及风险管理策略的组成相关方之一。

- **整体市场：**随着时间的推移，OTTF 工作产品的广泛应用与/或参考可按照促进信赖、责任感及全球创新的方式，帮助巩固全球信息技术设施的安全性。

## 总体实施方法

1、准备阶段：

**准备分析：**atsec 顾问将与机构协同工作，提供 O-TTPS 标准和认证体系的介绍。通过与机构关键岗位进行会谈，我们将帮助识别不符合该标准的主要差距，并帮助制定成功完成该认证的合理战略。

**实施选择准则申请（ISCA：Implementation Selection Criteria Application）：确**定认证范围，完成 ISCA 模板。

**证据整理和完善：**收集整理认证所需的证据，该证据将用于提供给 O-TTPS 认可评估机构。

**O-TTPS 培训：**atsec 可以为机构提供相关的技术培训。

2、认证阶段：

atsec 作为国际开放标准组织 O-TTPS 认证体系的授权认可的评估机构，将执行认证体系所规定的如下评估活动：

- 审核所提交的认证包是否符合 O-TTPS 要求
- 基于机构提供的证据执行评估
- 基于成功评估结果向认证授权（Accreditation Authority）机构提出通过认证的建议

正确的实现合规，该标准能够减少整个 COTS ICT 产品生命周期中获取恶意污染或假冒伪劣产品的风险，产品生命周期包括如下阶段：设计（design）、采购（sourcing）、构造（build）、实施（fulfillment）、分发（distribution）、维护（sustainment）和处置（disposal）。自愿性 O-TTPS 认证体系的符合性的展示提供了机构符合该业界标准的正式的认可，并且允许机构声明其为可信技术提供商 Open Trusted Technology Provider TM。

更多信息可以参见 atsec 网站信息：http://www.atsec.cn/cn/o-ttps.html

[1] Open Group 的认证图标是商标，且 The Open Group 是国际开放标准组织（The Open Group）的注册商标

[2] 国际开放标准组织可信技术论坛（The Open Group Trusted Technology Forum，简称“OTTF”或“论坛”）是一项旨在邀请行业、政府及其他感兴趣的参与者共同推进本标准及其他 OTTF 可交付成果的全球行动。

[3] atsec 信息安全是开放标准组织 O-TTPS 认证体系注册认可评估机构