OPEN TRUSTED TECHNOLOGY PROVIDER™ STANDARD (O-TTPS) CERTIFICATION PROGRAM

ORGANIZATIONAL SPECIFICS

Standards Organizations:	The Open Group
Technical Committees:	
Other Partnering Organizations:	
Government Organizations:	Department of Defense (DoD), Department of Homeland Security (DHS), National Aeronautics and Space Administration (NASA)
Industry Sector(s) / Technology:	ICT
Program / Activity Website URL(s):	O-TTPS https://ottps-cert.opengroup.org/

STANDARDS DRIVEN PUBLIC-PRIVATE PARTNERSHIP (PPP) OBJECTIVES

PPP Drivers:

The Open Trusted Technology Provider™ Standard (O-TTPS) was established to address growing supply chain security concerns from U.S. Department of Defense (DoD), U.S. Department of Homeland Security (DHS) as well as the private sector for integrity and security in technology supply chains.

PPP Goals:

The Open Trusted Technology Forum (OTTF), formed under The Open Group, brings together major industry representatives along with governmental entities. This collaboration aims to create and implement standards focused on supply chain security to establish a unified view of practicing supply chain risk management (SCRM) for information and communication technology (ICT) products. The OTTF focuses on mitigating risks from counterfeit and maliciously tainted products by establishing best practices and certification programs. These efforts ensure that organizations conform to stringent standards for maintaining the security and integrity of their supply chains.

Public Sector Role & Participation:

The Open Group serves as a neutral facilitator and brings together private sector entities as well as government to discuss their needs. In this model, all participants contributed on an equal level to develop standards. The OTTF remains an active group where members can continually discuss their issues and revise the standards and supporting materials as needed.

Government representatives engage in The Open Group activities through direct-participation, the same way any other stakeholder participates. Additionally, NASA sits on The Open Group's Governing Board. Moreover, the US government was instrumental in providing sponsorship to establish the O-TTPS as an International Standard as ISO 20243.

The Open Group is a membership-based consortia group. Membership is based on the revenue of the member and whether the organization is a technology vendor or end user. There are also membership options for academic institutions and government organizations.

The OTTF meets regularly, based on participating member preferences and availability, to continue iterating the O-TTPS, develop additional guidance and supporting materials, and collaborate with other forums of The Open Group.

Implementation Methods:

The OTTF provided a vendor-neutral collaborative environment (through forums and working groups) where technology vendors, government agencies, and other stakeholders could come together to develop and refine standards. This environment facilitated the creation of a unified voice to address supply chain security issues and to influence international standards and policy initiatives.

Industry experts and government representatives worked together within the OTTF to develop the O-TTPS. This process involved identifying and codifying best practices for securing the ICT supply chain, covering all stages of a product's lifecycle from design through disposal. This full lifecycle approach is also reflected in the O-TTPS Certification Program. The partnership established a certification program allowing organizations to be accredited as Open Trusted Technology Providers™. This program involves independent assessments by recognized third-party assessors to ensure conformance to the O-TTPS standard. The accreditation process is designed to be rigorous and transparent, providing assurance to customers about the integrity of certified providers.

Measurement of Success:

The first version of O-TTPS was published in April 2013, with Version 1.1 following in July 2014. This version was later approved by ISO/IEC in 2015 as ISO/IEC 20243:2015 Information technology — Open Trusted Technology Provider^{TM} Standard (O-TTPS) - Open Trusted Technology Provider^{TM} Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products. The 2023 version is the current version.

The O-TTPS has been widely adopted by major technology providers and integrators, enhancing the overall security of the technology supply chain. This broad adoption demonstrates the effectiveness of the standard in meeting industry needs and its alignment with both government and private sector requirements.

Government agencies, including the Department of Defense (DoD) support and endorse the standard. For instance, the National Defense Authorization Act (NDAA) for Fiscal Year 2016 required the assessment of O-TTPS or similar standards for procurement of secure information technology and cybersecurity systems. In many cases today, an organization or company if required to submit proof of certification for government procurement and/or contracts.

In February 2014, The Open Group launched the O-TTPS Certification Program, ensuring the Program complies with requirements dictated by the NIST NVLAP. This program allows organizations to certify their conformance to the O-TTPS standard, which helps assure customers of the integrity and security of commercial off-the-shelf (COTS) information and ICT products. The certification process involves independent assessment by recognized assessors, ensuring that applicants meet the stringent requirements set out in the standard.

Also, during the COVID-19 pandemic, there was an increase in O-TTPS certifications when many people worked from home and employers needed assurance that their systems were secure.

Key Takeaways:

In this instance, as government was a customer and a participant, industry was able to produce a standard that was practical for both the public and private sector and not customized for government only needs.

With support and active participation from the U.S. government, the OTTF was able to produce an International Standard and certification program.

Advice for Others:

Established standards development organizations (SDOs) and consortia already have procedures and infrastructure in place to foster collaboration. All parties involved (public and private sector entities) can focus on the technical aspects of the standards instead of developing procedures on how to write the documents and gather consensus.

Last updated September 2024. This use case was developed as part of an ANSI project performed under the following financial assistance award 70NANB24H075 from U.S. Department of Commerce, National Institute of Standards and Technology.