INTERNATIONAL STANDARD

ISO/IEC 20243

First edition
2015-09-15

Information Technology — Open Trusted Technology ProviderTM Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products

Technologies de l'information — Norme de fournisseur de technologie de confiance ouverte (O-TTPS) — Atténuation des produits contrefaits et malicieusement contaminés

Reference number
ISO/IEC 20243:2015(E)

© ISO/IEC 2015



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

1 Introduction 1
1.1 Objectives 1
1.2 Overview 1
1.3 Conformance 3
1.4 Terminology 3
1.5 Future Directions 4

2 Business Context and Overview 5
2.1 Business Environment Summary 5
2.1.1 Operational Scenario 5
2.2 Business Rationale 7
2.2.1 Business Drivers 7
2.2.2 Objectives and Benefits 8
2.3 Recognizing the COTS ICT Context 9
2.4 Overview 11
2.4.1 O-TTPF Framework Overview 11
2.4.2 Standard Overview 11
2.4.3 Relationship with Other Standards 12

3 O-TTPS – Tainted and Counterfeit Risks 13

4 O-TTPS – Requirements for Addressing the Risks of Tainted and Counterfeit Products 15
4.1 Technology Development 16
4.1.1 PD: Product Development/Engineering Method 16
4.1.1.1 PD_DES: Software/Firmware/Hardware Design Process 16
4.1.1.2 PD_CFM: Configuration Management 17
4.1.1.3 PD_MPP: Well-defined Development/Engineering Method Process and Practices 17
4.1.1.4 PD_QAT: Quality and Test Management 17
4.1.1.5 PD_PSM: Product Sustainment Management 18
4.1.2 SE: Secure Development/Engineering Method 18
4.1.2.1 SE_TAM: Threat Analysis and Mitigation 18
4.1.2.2 SE_RTP: Run-time Protection Techniques 19
4.1.2.3 SE_VAR: Vulnerability Analysis and Response 19
4.1.2.4 SE_PPR: Product Patching and Remediation 20
4.1.2.5 SE_SEP: Secure Engineering Practices 20

© ISO/IEC 2015 – All rights reserved

4.1.2.6 SE_MTL: Monitor and Assess the Impact of Changes in the Threat Landscape 20
4.2 Supply Chain Security 21
4.2.1 SC: Supply Chain Security 21
4.2.1.1 SC_RSM: Risk Management 21
4.2.1.2 SC_PHS: Physical Security 22
4.2.1.3 SC_ACC: Access Controls 22
4.2.1.4 SC_ESS: Employee and Supplier Security and Integrity 23
4.2.1.5 SC_BPS: Business Partner Security 23
4.2.1.6 SC_STR: Supply Chain Security Training 24
4.2.1.7 SC_ISS: Information Systems Security 24
4.2.1.8 SC_TTC: Trusted Technology Components 24
4.2.1.9 SC_STH: Secure Transmission and Handling 25
4.2.1.10 SC_OSH: Open Source Handling 25
4.2.1.11 SC_CTM: Counterfeit Mitigation 26
4.2.1.12 SC_MAL: Malware Detection 26

List of Tables

Table 1: O-TTPS Constituents and their Roles 6
Table 2: Threat Mapping 14

List of Figures

Figure 1: Constituents 6
Figure 2: Product Life Cycle – Categories and Activities 15

© ISO/IEC 2015 – All rights reserved

Preface

The Open Group

The Open Group is a global consortium that enables the achievement of business objectives through IT standards. With more than 400 member organizations, The Open Group has a diverse membership that spans all sectors of the IT community – customers, systems and solutions suppliers, tool vendors, integrators, and consultants, as well as academics and researchers – to:

- Capture, understand, and address current and emerging requirements, and establish policies and share best practices
- Facilitate interoperability, develop consensus, and evolve and integrate specifications and open source technologies
- Offer a comprehensive set of services to enhance the operational efficiency of consortia
- Operate the industry's premier certification service

Further information on The Open Group is available at www.opengroup.org.

The Open Group publishes a wide range of technical documentation, most of which is focused on development of Open Group Standards and Guides, but which also includes white papers, technical studies, certification and testing documentation, and business titles. Full details and a catalog are available at www.opengroup.org/bookstore.

Readers should note that updates – in the form of Corrigenda – may apply to any publication. This information is published at www.opengroup.org/corrigenda.

This Document

The Open Group Trusted Technology Forum (OTTF or Forum) is a global initiative that invites industry, government, and other interested participants to work together to evolve this Standard and other OTTF deliverables.

This Standard is the Open Trusted Technology Provider Standard (O-TTPS). The Standard has been developed by the OTTF and approved by The Open Group, through The Open Group Company Review process. There are two distinct elements that should be understood with respect to this Standard: the O-TTPF (Framework) and the O-TTPS (Standard).

The O-TTPF (Framework): The Framework is an evolving compendium of organizational guidelines and best practices relating to the integrity of Commercial Off-the-Shelf (COTS) Information and Communication Technology (ICT) products and the security of the supply chain throughout the entire product life cycle. An early version of the Framework was published as a White Paper in February 2011 (see Referenced Documents). The Framework serves as the basis for this Standard, future updates, and additional standards. The content of the Framework is the result of industry collaboration and research as to those commonly used commercially

© ISO/IEC 2015 – All rights reserved

reasonable practices that increase product integrity and supply chain security. The members of the OTTF will continue to collaborate with industry and governments and update the Framework as the threat landscape changes and industry practices evolve.

The O-TTPS (Standard): The O-TTPS is an open standard containing a set of guidelines that when properly adhered to have been shown to enhance the security of the global supply chain and the integrity of COTS ICT products. It provides a set of guidelines, requirements, and recommendations that help assure against maliciously tainted and counterfeit products throughout the COTS ICT product life cycle encompassing the following phases: design, sourcing, build, fulfillment, distribution, sustainment, and disposal.

Using the guidelines documented in the Framework as a basis, the OTTF is taking a phased approach and staging O-TTPS releases over time. This staging will consist of standards that focus on mitigating specific COTS ICT risks from emerging threats. As threats change or market needs evolve, the OTTF intends to update the O-TTPS (Standard) by releasing addenda to address specific threats or market needs.

The Standard is aimed at enhancing the integrity of COTS ICT products and helping customers to manage sourcing risk. The authors of this Standard recognize the value that it can bring to governments and commercial customers worldwide, particularly those who adopt procurement and sourcing strategies that reward those vendors who follow the O-TTPS best practice requirements and recommendations.

Note: Any reference to “providers” is intended to refer to COTS ICT providers. The use of the word “component” is intended to refer to either hardware or software components.

Intended Audience

This Standard is intended for organizations interested in helping the industry evolve to meet the threats in the delivery of trustworthy COTS ICT products. It is intended to provide enough context and information on business drivers to enable its audience to understand the value in adopting the guidelines, requirements, and recommendations specified within. It also allows providers, suppliers, and integrators to begin planning how to implement the Standard in their organizations. Additionally, acquirers and customers can begin recommending the adoption of the Standard to their providers and integrators.

© ISO/IEC 2015 – All rights reserved

Trademarks

ArchiMate®, DirecNet®, Jericho Forum®, Making Standards Work®, OpenPegasus®, The Open Group®, TOGAF®, and UNIX® are registered trademarks and Boundaryless Information Flow™, Build with Integrity Buy with Confidence™, Dependability Through Assuredness™, FACE™, Open Platform 3.0™, Open Trusted Technology Provider™, and The Open Group Certification Mark™ are trademarks of The Open Group.

All other brands, company, and product names are used for identification purposes only and may be trademarks that are the sole property of their respective owners.

© ISO/IEC 2015 – All rights reserved

Acknowledgements

The Open Group acknowledges the contribution of the following people and organizations in the development of this Standard (presented in alphabetical order).

In particular we would like to provide a special thank you and acknowledgement to the Chair and Vice Chair of the OTTF: Andras Szakal, IBM (Chair) and Edna Conway, Cisco Systems (Vice Chair).

The contributing members of The Open Group Trusted Technology Forum (OTTF):

Contributors	Organization
Jon Amis	Dell, Inc.
Paul Aschwald	Hewlett-Packard Company
Nadya Bartol	(formerly of) Booz Allen Hamilton
James Bean	Juniper Networks
Kristen Baldwin	US DoD AT&L
Terry Blevins	MITRE
Joshua Brickman	CA Technologies
Stan Brown	CA Technologies
Ben Calloni	Lockheed Martin
Suresh Cheruserri	(formerly of) Tata Consultancy Services
YouHong (Robert) Chu	Kingdee Software
Erv Comer	Motorola Solutions
Erin Connor	Electronic Warfare Associates (EWA) – Canada Ltd.
Tammy Compton	(formerly of) SAIC
Edna Conway	Cisco Systems Inc. OTTF Vice-Chair
Don Davidson	DOD-CIO
Mary Ann Davidson	Oracle Corporation
Charles Dekle	(formerly of) US DoD AT&L
Terrie Diaz	Cisco Systems Inc.
Robert Dix	Juniper Networks
Holly Dunlap	Raytheon Company
Bob Ellison	SEI
Marcus Fedeli	(formerly of) NASA

© ISO/IEC 2015 – All rights reserved

Contributors	Organization
Luke Forsyth	CA Technologies
Susan Fultz	Hewlett-Packard Company
Steve Goldberg	(formerly of) Motorola Solutions
Tim Hahn	IBM Corporation
Wes Higaki	Apex Assurance Group
Ken Hong Fong	(formerly of) US DoD AT&L
Helmut Kurth	atsec information security
Mike Lai	Microsoft Corporation
David Ling	Hewlett-Packard Company
Steve Lipner	Microsoft Corporation O-TTPF Work Stream Co-Chair
Dr. David McQueeney	IBM Corporation
Jim Mann	Hewlett-Packard Company
Al Marshall	NASA
Michele Moss	Booz-Allen Hamilton
Shawn Mullen	IBM Corporation
Fiona Pattinson	atsec information security
Brendan Peter	CA Technologies
Glenn Pittaway	Microsoft Corporation
Andy Purdy	Huawei Technologies
Dan Reddy	EMC Corporation
Karen Richter	IDA
Jim Robinson	Hewlett-Packard Company
Hart Rossman	(formerly of) SAIC
Mark Schiller	(formerly of) Hewlett-Packard Company
Thomas Stickels	MITRE
Andras R. Szakal	IBM Corporation OTTF Chair and O-TTPF Work Stream Co-Chair
Steve Whitlock	The Boeing Company
Jim Whitmore	IBM Corporation
Robert Williamson	SAIC
Eric Winterton	Booz Allen Hamilton
Joanne Woytek	NASA
Chee Wai Foong	Cisco Systems Inc.

© ISO/IEC 2015 – All rights reserved

The individuals providing early contributions to this work:

Contributor	Name
Randy Barr	Qualys
Rance DeLong	LynuxWorks
Chris Fagan	(formerly of) Microsoft Corporation
Rob Hoffman	High Assurance Systems, Inc.
Dave McDermitt	(formerly of) SAIC
Terry Morgan	(formerly of) Cisco Systems Inc.
Paul Nicholas	Microsoft Corporation
Kerri Patterson	(formerly of) Cisco Systems Inc.
Steve Venema	The Boeing Company
Larry Wagoner	NSA

The Open Group staff:

Name	Role
James Andrews	The Open Group Conformance Quality Manager
Joe Bergmann	Open Group Government Relations, Director, RT&ES
James de Raeve	VP Certification
Cathy Fox	Technical Editor
Jim Hietala	VP Security
Andrew Josey	Director, Standards
Sally Long	Director, The Open Group Trusted Technology Forum (OTTF)
Dave Lounsbury	Chief Technical Officer

© ISO/IEC 2015 – All rights reserved

Referenced Documents

The following documents are referenced in this Standard:

- 2007 Defense Science Board Task Force on Mission Impact of Foreign Influence on DoD Software, September 2007; findings and recommendations located at: www.acq.osd.mil/dsb/reports/ADA486949.pdf.
- Electronic Industry Citizenship Coalition (EICC) Code of Conduct; refer to: www.eicc.info.
- ISO/IEC 15408: Information Technology – Security Techniques – Evaluation Criteria for IT Security (Common Criteria).
- ISO/IEC 27000:2009: Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary.
- ISO/IEC Directives, Part 2: Rules for the Structure and Drafting of International Standards.
- NIST 800-12: An Introduction to Computer Security: The NIST Handbook.
- White Paper: Open Trusted Technology Provider Framework (O-TTPF), W113, published by The Open Group, February 2011; refer to: www.opengroup.org/bookstore/catalog/w113.htm.

© ISO/IEC 2015 – All rights reserved

1 Introduction

This chapter introduces this Standard – the Open Trusted Technology Provider Standard (O-TTPS) – and the normative terminology that should be understood in relation to specific requirements and recommendations found in Chapter 4 of this document.

1.1 Objectives

The Open Trusted Technology Provider Standard (O-TTPS) is a set of guidelines, requirements, and recommendations that, when practically applied, create a business benefit in terms of reduced risk of acquiring maliciously tainted or counterfeit products for the technology acquirer. Documenting best practices that have been taken from the experience of mature industry providers, rigorously reviewed through a consensus process, and established as requirements and recommendations in this Standard, can provide significant advantage in establishing a basis to reduce risk. A commitment by technology providers, large and small, suppliers of hardware and software components, and integrators to adopt this Standard is a commitment to using specific methodologies to assure the integrity of their hardware or software Commercial Off-the-Shelf (COTS) Information and Communication Technology (ICT) products. This Standard is detailed and prescriptive enough to be useful in raising the bar for all providers and lends itself to an accreditation process to provide assurance that it is being followed in a meaningful and repeatable manner.

1.2 Overview

This Standard (O-TTPS) is a set of guidelines, requirements, and recommendations that address specific threats to the integrity of hardware and software COTS ICT products throughout the product life cycle. This initial release of the Standard addresses threats related to maliciously tainted and counterfeit products.

The provider's product life cycle includes the work it does designing and developing products, as well as the supply chain aspects of that life cycle, collectively extending through the following phases: design, sourcing, build, fulfillment, distribution, sustainment, and disposal. While this Standard cannot fully address threats that originate wholly outside any span of control of the provider – for example, a counterfeiter producing a fake printed circuit board assembly that has no original linkage to the Original Equipment Manufacturer (OEM) – the practices detailed in the Standard will provide some level of mitigation. An example of such a practice would be the use of security labeling techniques in legitimate products.

The two major threats that acquirers face today in their COTS ICT procurements, as addressed in this Standard, are defined as:

1. Maliciously tainted product – the product is produced by the provider and is acquired through a provider's authorized channel, but has been tampered with maliciously.

© ISO/IEC 2015 – All rights reserved

2. Counterfeit product – the product is produced other than by, or for, the provider, or is supplied to the provider by other than a provider's authorized channel and is presented as being legitimate even though it is not.

Note: All instances, within this standard, of the use of the words: taint, tainted, tainting, refer to maliciously taint, maliciously tainted, and maliciously tainting, respectively.

Trusted Technology Providers manage their product life cycle, including their extended supply chains, through the application of defined, monitored, and validated best practices. The product's integrity is strengthened when providers and suppliers follow the requirements and recommendations specified in this Standard. The industry consensus reflected here and in the Open Trusted Technology Provider Framework (O-TTPF) draws from the following areas that are integral to product integrity: product development/engineering, secure development/engineering, and supply chain security. Additionally, product integrity and supply chain security are enhanced by following practices among suppliers, trading partners, providers, and, when appropriate, acquiring customers to preserve the product's intended configuration.

This Standard is focused on the security of the supply chain *versus* the business management aspects of the supply chain. This Standard takes a comprehensive view about what providers should do in order to be considered a Trusted Technology Provider that "builds with integrity". This includes practices that providers incorporate in their own internal product life cycle processes, that portion of product development that is "in-house" and over which they have more direct operational control. Additionally, it includes the provider's supply chain security practices that need to be followed when incorporating third-party hardware or software components, or when depending on external manufacturing and delivery or supportive services.

The Standard makes a distinction between provider and supplier. Suppliers are those upstream vendors who supply components or solutions (software or hardware) to providers or integrators. Providers are those vendors who supply COTS ICT products directly to the downstream integrator or acquirer.

Ideally, the guidelines, requirements, and recommendations included in this Standard will be widely adopted by providers and their suppliers regardless of size and will provide benefits throughout the industry.

For this version of the Standard, the following elements are considered out of scope:

- This Standard does not focus on guidelines, requirements, and recommendations for the acquirer. The Forum is considering addressing this area in subsequent versions of the Standard. In the meantime, an acquirer does have a role to play in assuring that the products and components they procure are built with integrity. One of the ways that the acquirer can do that is to require their providers, suppliers, and integrators to be Trusted Technology Providers. Another way is to not knowingly support the "grey market", realizing that if an acquirer elects to receive hardware or software support from grey market suppliers, it is at their own risk and generally outside of the influence of the legitimate provider.
- This Standard is not meant to be comprehensive as to all practices that a provider should follow when building software or hardware. For a more comprehensive set of foundational

© ISO/IEC 2015 – All rights reserved

best practices that a provider could implement to produce good quality products, readers can refer to the O-TTPF White Paper.

- This version of the Standard does not apply to the operation or hosting infrastructure of on-line services, but can apply to COTS ICT products in as far as they are utilized by those services.

This Standard complements existing standards covering product security functionality and product information assurance, such as ISO/IEC 15408 (Common Criteria).

1.3 Conformance

The OTTF intends to develop conformance criteria and create an Accreditation Policy and Program for the Open Trusted Technology Provider Standard (O-TTPS) as a useful tool for all constituents with an interest in supply chain security. Without the associated conformance criteria and an Accreditation Program, there is no assurance that an organization has implemented practices according to the O-TTPS.

Accreditation will provide formal recognition of conformance to the O-TTPS, which allows:

- Providers and practitioners to make and substantiate clear claims of conformance to the Standard
- Acquirers to specify and successfully procure from providers who conform to the Standard

Conformance assessment is the act of determining the conformance of an implementation to a specification, or the adherence of a business operation to a best practice or process definition. There are many techniques for assessing such conformance, including the use of a standardized test method, quality assessment by industry experts or third-party test laboratories, and vendors' claims of conformance made within a defined legal framework.

The O-TTPS accreditation process, conformance criteria, conformance assessment, policies, parties, and their roles will be defined and approved after the publication of Version 1.0 of this Standard.

1.4 Terminology

This section provides a set of terms and their definitions, which should be used when describing and interpreting the Standard requirements and recommendations specified in Chapter 4 of this Standard. These terms are aligned with ISO/IEC Directives, Part 2 (Annex H).

Shall	Indicates an absolute, mandatory requirement of the Standard that has to be implemented in order to conform to the Standard and from which no deviation is permitted. Do not use "must" as an alternative for "shall". (This will avoid any confusion between the requirements of a document and external statutory obligations.)

© ISO/IEC 2015 – All rights reserved