THE OPEN GROUP SERIES

O-TTPS for ICT Product Integrity and Supply Chain Security

A Management Guide

Van Haren PUBLISHING

THE Open GROUP

O-TTPS FOR ICT PRODUCT INTEGRITY AND SUPPLY CHAIN SECURITY

A MANAGEMENT GUIDE

The Open Group Publications available from Van Haren Publishing

The TOGAF Series:
TOGAF® Version 9.1
TOGAF® Version 9.1 – A Pocket Guide
TOGAF® 9 Foundation Study Guide, 3rd Edition
TOGAF® 9 Certified Study Guide, 3rd Edition

The Open Group Series:
The IT4IT™ Reference Architecture, Version 2.0
IT4IT™ for Managing the Business of IT – A Management Guide
IT4IT™ Foundation Study Guide
The IT4IT™ Reference Architecture, Version 2.0 – A Pocket Guide
Cloud Computing for Business – The Open Group Guide
ArchiMate® 2.1 – A Pocket Guide
ArchiMate® 2.1 Specification
ArchiMate® 2 Certification – Study Guide
ArchiMate® 3.0 Specification

The Open Group Security Series:
O-TTPS - A Management Guide
Open Information Security Management Maturity Model (O-ISM3)
Open Enterprise Security Architecture (O-ESA)
Risk Management – The Open Group Guide
The Open FAIR™ Body of Knowledge – A Pocket Guide

All titles are available to purchase from:
www.opengroup.org
www.vanharen.net
and also many international and online distributors.

O-TTPS for ICT Product Integrity and Supply Chain Security

A Management Guide

Using the Open Trusted Technology Provider™ Standard
(O-TTPS) (ISO/IEC 20243:2015) and the Certification Program

Title:	O-TTPS for ICT Product Integrity and Supply Chain Security – A Management Guide
Series:	The Open Group Series
A Publication of:	The Open Group
Authors:	Sally Long and Members of The Open Group Trusted Technology Forum (OTTF)
Publisher:	Van Haren Publishing, Zaltbommel, www.vanharen.net
ISBN Hardcopy:	978 94 018 0092 1
ISBN eBook:	978 94 018 0093 8
ISBN ePub:	978 94 018 0094 5
Edition:	First edition, first impression, January 2017
Layout and Cover Design:	CO2 Premedia, Amersfoort – NL

O-TTPS for ICT Product Integrity and Supply Chain Security – A Management Guide
Document Number: G169
Published by The Open Group, January 2017
Comments relating to the material contained in this document may be submitted to:
The Open Group
Apex Plaza
Reading
Berkshire, RG1 1AX
United Kingdom
or by electronic mail to: ogpubs@opengroup.org

Contents

Preface

The Open Group

The Open Group is a global consortium that enables the achievement of business objectives through IT standards. With more than 500 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, 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.

About The Open Group Trusted Technology Forum (OTTF) (the Forum)

The Forum, established under The Open Group in December 2010, is an organized collaboration among representatives from government, academia, and the IT industry. It develops and maintains the Open Trusted Technology Provider™ Standard – Mitigating Maliciously Tainted and Counterfeit Products (O-TTPS), also known as ISO/IEC 20243:2015. The mission of the Forum is

to create and drive the adoption of the O-TTPS, the O-TTPS Certification Program, and other Forum deliverables.

For more information on the Forum, visit www.opengroup.org/subjectareas/trusted-technology.

About the O-TTPS Standard

The O-TTPS (and its equivalent ISO/IEC 20243:2015) is an open standard containing a set of requirements that when properly adhered to have been shown to enhance the security of the global supply chain and the integrity of commercial off-the-shelf (COTS) information and communication technology (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, which includes the supply chain.

This Document

This Management Guide provides guidance on why a technology provider company should consider adopting O-TTPS and becoming certified; what they should understand about the Certification Program; and how they can best prepare for the process once they decide to pursue certification.

It is designed to offer guidance to managers – business managers, procurement managers, or program managers – who are considering becoming a certified Open Trusted Technology Provider™. Additionally, it provides an overview of the certification process, with pointers to the relevant supporting documents, offering a practical introduction to executives, managers, those involved directly in implementing the best practices defined in the Standard, and those who would provide the Evidence of Conformance to the best practice requirements for certification.

As the O-TTPS Certification Program is open to all constituents involved in a product's life cycle – from design through disposal – including those in the product's supply chain, this Management Guide should be of interest to all ICT customers as well as ICT providers (e.g., Original Equipment Manufacturers

(OEMs), Original Design Manufactures (ODMs), integrators, hardware or software component suppliers, value-add distributors, and resellers).

This Management Guide is structured as follows:

- Chapter 1 (Introduction) provides an executive summary, an overview of the threats and risks, some background information, a brief introduction to the Standard and the Certification Program, and a business rationale for getting certified as an Open Trusted Technology Provider.
- Chapter 2 (The Standard) gives an overview of the Standard and the categorization of the best practices that are required throughout the full product life cycle of a product. This chapter is an introduction to the structure of the Standard; the full set of requirements and recommendations in the Standard can be found in Appendix A.
- Chapter 3 (Organizing and Preparing for Certification) offers practical steps and best practices that will help an organization prepare and properly structure their approach for certification to best effect.
- Chapter 4 (The Certification Process) describes the certification processes. The information in this chapter should allow an organization to understand the basics of what is required to progress through the certification process. One of the first decisions the organization being certified should make is to decide on the type of assessment that best fits their business needs. The two options are: Self-Assessed and Third-Party Assessed.
- Chapter 5 (Self-Assessed Certification Process) covers the process for the Self-Assessed tier of the O-TTPS Certification Program in more detail.
- Chapter 6 (Third-Party Assessed Certification Process) covers the process for the Third-Party Assessed tier of the O-TTPS Certification Program in more detail.
- Chapter 7 (Summary of the Certification Steps) provides a list of the certification process steps as a summary, which can be found in more detail in the Certification Policy. Section 7.1 provides a summary of the steps for the Self-Assessed tier and Section 7.2 provides a summary of the steps for the Third-Party Assessed tier.
- Appendix A (O-TTPS Requirements) is a replica of the Terminology section (Section 1.4) of the Standard (i.e., O-TTPS Version 1.1, which is technically equivalent to ISO/IEC 20243:2015) that defines the prescriptive terms used in Chapter 4 of the Standard, which defines the requirements and recommendations for mitigating the risk of tainted and counterfeit products.

- Appendix B (Additional Resources) contains additional resources and references that provide useful information about the Forum, the O-TTPS, the O-TTPS Certification Program, and the Forum's other deliverables.

Conventions Used in this Management Guide

The following conventions are used throughout this Management Guide in order to help identify important information and avoid confusion over the intended meaning.

- The Standard
  Throughout this document when "the Standard" is used it should be interpreted as referring to both the O-TTPS and ISO/IEC 20243:2015, as they are technically equivalent. The Certification Program is applicable to both.
- Ellipsis (…)
  Indicates a continuation; such as an incomplete list of example items, or a continuation from preceding text.
- **Bold**
  Used to highlight specific terms.
- *Italics*
  Used for emphasis. May also refer to other external documents.

Trademarks

ArchiMate®, DirecNet®, Making Standards Work®, OpenPegasus®, The Open Group®, TOGAF®, UNIX®, UNIXWARE®, X/Open®, and the Open Brand X® logo are registered trademarks and Boundaryless Information Flow™, Build with Integrity Buy with Confidence™, Dependability Through Assuredness™, EMMM™, FACE™, the FACE™ logo, IT4IT™, the IT4IT™ logo, O-DEF™, O-PAS™, Open FAIR™, Open Platform 3.0™, Open Process Automation™, Open Trusted Technology Provider™, Platform 3.0™, SOSA™, the Open O™ logo, and The Open Group Certification logo (Open O and check™) 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.

Acknowledgements

The Open Group gratefully acknowledges the following contributors in the development of this Management Guide:

- Past and present members of The Open Group Trusted Technology Forum (OTTF) for developing the Standard, the O-TTPS Certification Program, and the additional associated published documents. Those member companies include: atsec information security, Boeing, Booz Allen Hamilton, Carnegie Mellon University – Software Engineering Institute, Cisco Systems Inc., CyberCore Technologies, Dell, EMC, EWA-Canada, Huawei, Hewlett-Packard, IBM, Interos Solutions, Microsoft, MITRE, NASA, NTG, Oracle, Office of the Under Secretary of Defense for Acquisition/Technology and Logistics (OUSD AT&L), PCi Tec, Quinsigamond Community College, Strategic Communications, TaTa Consulting Services, and the US Department of Defense/CIO.
- The following contributors and reviewers:
  - Jon Amis, Dell Technologies
  - Erin Connor, EWA-Canada
  - Edna Conway, Cisco Systems Inc.
  - Terrie Diaz, Cisco Systems Inc.
  - Mike Lai, Microsoft Corporation
  - Fiona Pattinson, atsec information security corporation
  - Andy Purdy, Huawei Technologies USA
  - Dan Reddy, Quinsigamond Community College, previously of EMC Corporation
  - Andras Szakal, IBM Corporation
  - Joanne Woytek, NASA
  - Sally Long, The Open Group

Referenced Documents

The documents listed below are referenced in this Management Guide and can be accessed from the O-TTPS Certification website (http://ottps-cert.opengroup.org).

The published documents referenced below should be considered the official documents for the Standard and Certification Program, and take precedence over any content otherwise mentioned in this Management Guide.

- Assessment Procedures
- Certification Agreement
- Certification Package Document, including the Assessment Report
- Certification Policy
- Conformance Requirements
- Conformance Statement
- Conformance Statement Questionnaire
- Implementation Selection Criteria Application (ISCA) Document
- O-TTPS Recognized Assessor Agreement
- Open Trusted Technology Provider™ Standard (O-TTPS) (also now known as ISO/IEC 20243:2015)
- Trademark License Agreement