INTERNATIONAL STANDARD

ISO/IEC 20243-1

Second edition
2023-11

Information technology — Open Trusted Technology Provider™ Standard (O-TTPS) —

Part 1: Requirements and recommendations for mitigating maliciously tainted and counterfeit products

Reference number
ISO/IEC 20243-1:2023(E)

© ISO/IEC 2023



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2023

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO/IEC 2023 – All rights reserved

Contents

Page

Foreword ... iv
Preface ... vi
Trademarks ... viii
Introduction ... ix
1 Scope ... 1
1.1 Conformance ... 2
1.2 Future Directions ... 2
2 Normative references ... 2
3 Terms and definitions ... 2
4 Business Context and Overview ... 9
4.1 Business Environment Summary ... 9
4.1.1 Operational Scenario ... 9
4.2 Business Rationale ... 11
4.2.1 Business Drivers ... 11
4.2.2 Objectives and Benefits ... 12
4.3 Recognizing the COTS ICT Context ... 13
4.4 Overview ... 14
4.4.1 O-TTPF Overview ... 14
4.4.2 O-TTPS Overview ... 15
4.4.3 Relationship with Other Standards ... 15
5 O-TTPS – Tainted and Counterfeit Risks ... 16
6 O-TTPS – Requirements for Addressing the Risks of Tainted and Counterfeit Products ... 17
6.1 Technology Development ... 18
6.1.1 PD: Product Development/Engineering Method ... 19
6.1.2 SE: Secure Development/Engineering Method ... 21
6.2 Supply Chain Security ... 24
6.2.1 SC: Supply Chain Security Method ... 24
Bibliography ... 31

© ISO/IEC 2023 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by The Open Group [as Open Trusted Technology Provider Standard (O-TTPS) V1.2, Part 1: Requirements and Recommendations] and drafted in accordance with its editorial rules. It was adopted, under the JTC 1 PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*.

This second edition cancels and replaces the first edition (ISO/IEC 20243-1:2018), which has been technically revised.

The main changes are as follows:

— Wording was changed throughout the document, including in beginning materials, attribute definitions and requirements, as necessary to improve clarity and/or concision.

— The definition of “component” has been clarified to include both hardware and software.

— A definition for “security-critical” has been added.

— PD_DES.01 has become a mandatory requirement.

— PD_CFM.04 has become a mandatory requirement.

— The attribute definition of PD_QAT has been clarified.

— The attribute definition of PD_PSM has been clarified.

 © ISO/IEC 2023 – All rights reserved

— The SE_VAR requirements have been largely reworked and reorganized, with a new mandatory requirement being added and several existing requirements becoming mandatory.

— SE_PPR.02 has become a mandatory requirement.

— SE_PPR.04 has become a mandatory requirement.

— SC_RSM.05 has become a mandatory requirement.

— SC_ACC.04 has become a mandatory requirement.

— SC_ESS.02 has become a mandatory requirement.

— SC_ESS.03 has become a mandatory requirement.

— SC_ESS.04 has been completely rewritten and has become a mandatory requirement.

— SC_BPS.02 has become a mandatory requirement.

— The SE_STH requirements have been largely reworked and reorganized, with a new requirement being added and an existing requirement becoming mandatory.

— SC_CTM.02 has been heavily revised and has become a mandatory requirement.

— SC_MAL.02 has been heavily revised and has become a mandatory requirement

A list of all parts in the ISO/IEC 20243 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

© ISO/IEC 2023 – All rights reserved

Preface

The Open Group

The Open Group is a global consortium that enables the achievement of business objectives through technology standards. With more than 870 member organizations, we have a diverse membership that spans all sectors of the technology community – customers, systems and solutions suppliers, tool vendors, integrators and consultants, as well as academics and researchers.

The mission of The Open Group is to drive the creation of Boundaryless Information Flow™ achieved by:

— Working with customers to capture, understand, and address current and emerging requirements, establish policies, and share best practices

— Working with suppliers, consortia, and standards bodies to develop consensus and facilitate interoperability, to evolve and integrate specifications and open source technologies

— Offering a comprehensive set of services to enhance the operational efficiency of consortia

— Developing and operating the industry's premier certification service and encouraging procurement of certified products

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 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/library.

This Document

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

This document is Part 1 of the Open Trusted Technology Provider Standard (O-TTPS). It 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 document: the O-TTPF (Framework) and the O-TTPS (Standard).

The O-TTPF (Framework): The O-TTPF is an evolving compendium of organizational guidelines and best practices relating to the integrity of Commercial Off-The-Shelf (COTS) Information and Communications Technology (ICT) products and the security of the supply chain throughout the entire product lifecycle.

An early version of the O-TTPF was published as a White Paper in February 2011, revised in November 2015, and has since been updated and published as a Guide in September 2021. The O-TTPF serves as the basis for the O-TTPS, future updates, and additional standards. The content of the O-TTPF is the result of industry collaboration and research as to those commonly used commercially 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 O-TTPF as the threat landscape changes and industry practices evolve.

 © ISO/IEC 2023 – All rights reserved

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. Part 1 of the O-TTPS (this document) provides a set of guidelines, requirements, and recommendations that help assure against maliciously tainted and counterfeit products throughout the COTS ICT product lifecycle encompassing the following phases: design, sourcing, build, fulfillment, distribution, sustainment, and disposal.

The O-TTPS, Part 2: Assessment Procedures for the O-TTPS provides assessment procedures that may be used to demonstrate conformance with the requirements provided in Clause 6 of this document.

Using the guidelines documented in the O-TTPF 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 by releasing addenda to address specific threats or market needs.

The O-TTPS is aimed at enhancing the integrity of COTS ICT products and helping customers to manage sourcing risk. The authors 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

The O-TTPS 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 O-TTPS in their organizations. Additionally, acquirers and customers can begin recommending the adoption of the O-TTPS to their providers and integrators.

© ISO/IEC 2023 – All rights reserved

Trademarks

ArchiMate, DirecNet, Making Standards Work, Open O logo, Open O and Check Certification logo, Platform 3.0, The Open Group, TOGAF, UNIX, UNIXWARE, and the Open Brand X logo are registered trademarks and Boundaryless Information Flow, Build with Integrity Buy with Confidence, Commercial Aviation Reference Architecture, Dependability Through Assuredness, Digital Practitioner Body of Knowledge, DPBoK, EMMM, FACE, the FACE logo, FHIM Profile Builder, the FHIM logo, FPB, Future Airborne Capability Environment, IT4IT, the IT4IT logo, O-AA, O-DEF, O-HERA, O-PAS, Open Agile Architecture, Open FAIR, Open Footprint, Open Process Automation, Open Subsurface Data Universe, Open Trusted Technology Provider, OSDU, Sensor Integration Simplified, SOSA, and the SOSA logo 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 2023 – All rights reserved

Introduction

Part 1 of the 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 document, 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 document is a commitment to using specific methodologies to assure the integrity of their hardware or software Commercial Off-The-Shelf (COTS) Information and Communications Technology (ICT) products. This document is detailed and prescriptive enough to be useful in raising the bar for all providers and lends itself to the accompanying certification process that provides assurance that it is being followed in a meaningful and repeatable manner.

Part 1 of the O-TTPS (this document) 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 lifecycle. This version of the O-TTPS addresses threats related to maliciously tainted and counterfeit products.

The provider's product lifecycle includes the work it does designing and developing products, as well as the supply chain aspects of that lifecycle, collectively extending through the following phases: design, sourcing, build, fulfillment, distribution, sustainment, and disposal. While this document 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 this document 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 document, are defined as:

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

2. Counterfeit product – the product is produced other than by, or for, the provider, or it 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 document, of the use of the words: taint, tainted, tainting, refer to malicious taint, maliciously tainted, and malicious tainting, respectively.

Trusted Technology Providers manage their product lifecycle, 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 document. 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.

© ISO/IEC 2023 – All rights reserved

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

Part 1: Requirements and recommendations

1 Scope

This document is focused on the security of the supply chain *versus* the business management aspects of the supply chain. This document 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 lifecycle 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 document 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.

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

For this version of the O-TTPS, the following elements are considered out of scope:

— This document does not focus on guidelines, requirements, and recommendations for the acquirer; the OTTF is considering addressing this area in a separate, complementary publication, such as a Guide.

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

© ISO/IEC 2023 – All rights reserved

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

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

1.1 Conformance

The Open Group has developed and maintains conformance criteria, assessment procedures, and a Certification Policy and Program for the O-TTPS as a useful tool for all constituents with an interest in supply chain security.

The conformance requirements and assessment procedures are available in the O-TTPS, Part 2: Assessment Procedures for the O-TTPS.

Certification provides formal recognition of conformance to the O-TTPS, which allows:

— Providers and practitioners to make and substantiate clear claims of conformance to the O-TTPS

— Acquirers to specify and successfully procure from providers who conform to the O-TTPS

1.2 Future Directions

The OTTF intends to address possible additional threats and risks with best practice requirements and recommendations in a future version.

The OTTF intends to offer additional guidance for different classes of Trusted Technology Providers seeking certification against this document.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

Shall	Indicates an absolute, mandatory requirement that has to be implemented in order to conform to this document 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.)
Shall not	Indicates an absolute preclusion, and if implemented would represent a non-conformity. Do not use “may not” instead of “shall not” to express a prohibition.
Should	Indicates a recommendation among several possibilities that is particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required.

 © ISO/IEC 2023 – All rights reserved