INTERNATIONAL STANDARD

ISO/IEC 20243-2

Second edition
2023-11

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

Part 2: Assessment procedures for the O-TTPS

Reference number
ISO/IEC 20243-2:2023(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 ... 1
1.2 Future Directions ... 1
2 Normative references ... 1
3 Terms and definitions ... 2
4 General Concepts ... 3
4.1 The O-TTPS ... 3
4.2 Assessment Concepts: Relevance of Scope of Assessment and Selected Representative Products ... 4
4.3 Relevance of IT Technology Provider Categories in the Supply Chain ... 4
5 Assessment Requirements ... 5
5.1 General Requirements for Assessor Activities ... 5
5.1.1 General Requirements for Evidence of Conformance ... 5
6 Assessor Activities for O-TTPS Requirements ... 8
6.1 PD_DES: Software/Firmware/Hardware Design Process ... 9
6.2 PD_CFM: Configuration Management ... 10
6.3 PD_MPP: Well-Defined Development/Engineering Method Process and Practices ... 14
6.4 PD_QAT: Quality and Test Management ... 14
6.5 PD_PSM: Product Sustainment Management ... 16
6.6 SE_TAM: Threat Analysis and Mitigation ... 18
6.7 SE_VAR: Vulnerability Analysis and Response ... 20
6.8 SE_PPR: Product Patching and Remediation ... 23
6.9 SE_SEP: Secure Engineering Practices ... 25
6.10 SE_MTL: Monitor and Assess the Impact of Changes in the Threat Landscape ... 26
6.11 SC_RSM: Risk Management ... 28
6.12 SC_PHS: Physical Security ... 30
6.13 SC_ACC: Access Controls ... 31
6.14 SC_ESS: Employee and Supplier Security and Integrity ... 34
6.15 SC_BPS: Business Partner Security ... 36
6.16 SC_STR: Supply Chain Security Training ... 37
6.17 SC_ISS: Information Systems Security ... 38
6.18 SC_TTC: Trusted Technology Components ... 38
6.19 SC_STH: Secure Transmission and Handling ... 40
6.20 SC_OSH: Open Source Handling ... 42
6.21 SC_CTM: Counterfeit Mitigation ... 44
6.22 SC_MAL: Malware Detection ... 46
Annex A ASSESSMENT GUIDANCE ... 48
Annex B ASSESSMENT REPORT TEMPLATE ... 49
Bibliography ... 50

© 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 2: Assessment Procedures for the O-TTPS] 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 20243-2:2018), which has been technically revised.

The main changes are as follows:

— Wording has been changed throughout the document, including in introductory 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 revised heavily 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 2 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 (see Referenced Documents). 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 (see Referenced Documents) provides assessment procedures that may be used to demonstrate conformance with the requirements provided in Clause 6 of the O-TTPS, Part 1.

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 2 of the O-TTPS specifies the procedures to be utilized by an assessor when conducting a conformity assessment to the mandatory requirements in the O-TTPS.[1)]

These Assessment Procedures are intended to ensure the repeatability, reproducibility, and objectivity of assessments against the O-TTPS. Though the primary audience for this document is the assessor, an Information Technology (IT) provider who is undergoing assessment or preparing for assessment, may also find this document useful.

[1)] The O-TTPS Part 1 is freely available at: www.opengroup.org/library/c185-1.

© ISO/IEC 2023 – All rights reserved

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

Part 2:
Assessment procedures for the O-TTPS

1 Scope

The Assessment Procedures defined in this document are intended to ensure the repeatability, reproducibility, and objectivity of assessments against the O-TTPS. Though the primary audience for this document is the assessor, an Information Technology (IT) provider who is undergoing assessment or preparing for assessment, may also find this document useful.

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

Refer to the O-TTPS, Part 1: Requirements and Recommendations.

2 Normative references

There are no normative references in this document.

© ISO/IEC 2023 – All rights reserved