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

Part 2:
**Assessment procedures for the O-TTPS
and ISO/IEC 20243-1:2018**

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

*Partie 2: Procédures d'évaluation de l'O-TTPS et l'ISO/IEC 20243-
1:2018*





COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2018

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, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Published in Switzerland

Contents

1.	Introduction	1
1.1	Scope	1
1.2	Normative References	1
1.3	Terms and Definitions	1
1.3.1	Distributor	1
1.3.2	Evidence of Conformance	1
1.3.3	Implementation Evidence	1
1.3.4	O-TTPS Requirements	1
1.3.5	Organization	1
1.3.6	Pass-Through Reseller	2
1.3.7	Process Evidence	2
1.3.8	Scope of Assessment	2
1.3.9	Selected Representative Product	2
2.	General Concepts	3
2.1	The O-TTPS	3
2.2	Assessment Concepts: Relevance of Scope of Assessment and Selected Representative Products	3
2.3	Relevance of IT Technology Provider Categories in the Supply Chain	4
3.	Assessment Requirements	6
3.1	General Requirements for Assessor Activities	6
3.1.1	General Requirements for Evidence of Conformance	6
4.	Assessor Activities for O-TTPS Requirements	8
4.1	PD_DES: Software/Firmware/Hardware Design Process	8
4.2	PD_CFM: Configuration Management	9
4.3	PD_MPP: Well-defined Development/Engineering Method Process and Practices	11
4.4	PD_QAT: Quality and Test Management	11
4.5	PD_PSM: Product Sustainment Management	13
4.6	SE_TAM: Threat Analysis and Mitigation	14
4.7	SE_VAR: Vulnerability Analysis and Response	16
4.8	SE_PPR: Product Patching and Remediation	17
4.9	SE_SEP: Secure Engineering Practices	17
4.10	SE_MTL: Monitor and Assess the Impact of Changes in the Threat Landscape	19
4.11	SC_RSM: Risk Management	20
4.12	SC_PHS: Physical Security	21
4.13	SC_ACC: Access Controls	22
4.14	SC_ESS: Employee and Supplier Security and Integrity	23
4.15	SC_BPS: Business Partner Security	24
4.16	SC_STR: Supply Chain Security Training	24
4.17	SC_ISS: Information Systems Security	25
4.18	SC_TTC: Trusted Technology Components	25
4.19	SC_STH: Secure Transmission and Handling	26
4.20	SC_OSH: Open Source Handling	28
4.21	SC_CTM: Counterfeit Mitigation	29
4.22	SC_MAL: Malware Detection	30
A.1	Guidance	32

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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by The Open Group and was adopted, under the PAS procedure, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, in parallel with its approval by national bodies of ISO and IEC.

A list of all parts in the ISO 20243 series can be found on the ISO website.

1. Introduction

1.1 Scope

This document specifies the procedures to be utilized by an assessor when conducting a conformity assessment to the mandatory requirements in the Open Trusted Technology Provider™ Standard (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.

1.2 Normative References

The following documents, in whole or in part, are normatively referenced within this document. For undated references, the latest edition of the referenced document applies:

- ISO/IEC 20243-1:2018 Information Technology – Open Trusted Technology Provider™ Standard (O-TTPS) – Mitigating Maliciously Tainted and Counterfeit Products

¹ The O-TTPS is freely available at: www.opengroup.org/bookstore/catalog/c147.htm. The O-TTPS is technically identical to ISO/IEC 20243:2015 ISO/IEC 20243-1:2018 and is available at: www.iso.org