DRAFT INTERNATIONAL STANDARD

ISO/IEC DIS 22076

ISO/IEC JTC **1**

Secretariat: **ANSI**

Voting begins on:
2017-02-03

Voting terminates on:
2017-04-27

The open trusted technology provider standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products assessment procedures v1.1.1

Titre manque

ICS: 13.310; 35.030

This document is circulated as received from the committee secretariat.

FAST TRACK PROCEDURE

PUBLICLY AVAILABLE SPECIFICATON PROCEDURE

THIS DOCUMENT IS A DRAFT CIRCULATED FOR COMMENT AND APPROVAL. IT IS THEREFORE SUBJECT TO CHANGE AND MAY NOT BE REFERRED TO AS AN INTERNATIONAL STANDARD UNTIL PUBLISHED AS SUCH.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

Reference number
ISO/IEC DIS 22076:2017(E)

© ISO/IEC 2017



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2017, 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 4
   1.1 Scope 4
   1.2 Normative References 4
   1.3 Terms and Definitions 4
      1.3.1 Distributor 4
      1.3.2 Evidence of Conformance 4
      1.3.3 Implementation Evidence 4
      1.3.4 O-TTPS Requirements 4
      1.3.5 Organization 5
      1.3.6 Pass-Through Reseller 5
      1.3.7 Process Evidence 5
      1.3.8 Scope of Assessment 5
      1.3.9 Selected Representative Product 5
2. General Concepts 6
   2.1 The O-TTPS 6
   2.2 Assessment Concepts: Relevance of Scope of Assessment and Selected Representative Products 6
   2.3 Relevance of IT Technology Provider Categories in the Supply Chain 7
3. Assessment Requirements 9
   3.1 General Requirements for Assessor Activities 9
      3.1.1 General Requirements for Evidence of Conformance 9
4. Assessor Activities for O-TTPS Requirements 11
   4.1 PD_DES: Software/Firmware/Hardware Design Process 11
   4.2 PD_CFM: Configuration Management 12
   4.3 PD_MPP: Well-defined Development/Engineering Method Process and Practices 14
   4.4 PD_QAT: Quality and Test Management 15
   4.5 PD_PSM: Product Sustainment Management 16
   4.6 SE_TAM: Threat Analysis and Mitigation 18
   4.7 SE_VAR: Vulnerability Analysis and Response 19
   4.8 SE_PPR: Product Patching and Remediation 20
   4.9 SE_SEP: Secure Engineering Practices 21
   4.10 SE_MTL: Monitor and Assess the Impact of Changes in the Threat Landscape 22
   4.11 SC_RSM: Risk Management 23
   4.12 SC_PHS: Physical Security 25
   4.13 SC_ACC: Access Controls 26
   4.14 SC_ESS: Employee and Supplier Security and Integrity 27
   4.15 SC_BPS: Business Partner Security 28
   4.16 SC_STR: Supply Chain Security Training 28
   4.17 SC_ISS: Information Systems Security 29
   4.18 SC_TTC: Trusted Technology Components 29
   4.19 SC_STH: Secure Transmission and Handling 30
   4.20 SC_OSH: Open Source Handling 32
   4.21 SC_CTM: Counterfeit Mitigation 33
   4.22 SC_MAL: Malware Detection 34
A Annex: Assessment Guidance 36
   A.1 Guidance 36
B Annex: Assessment Report Template 37

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 20243:2015: Information Technology – Open Trusted Technology Provider™ Standard (O-TTPS) – Mitigating Maliciously Tainted and Counterfeit Products

1.3 Terms and Definitions

For the purposes of this document, the following terms and definitions apply. For terms not defined here refer to the Glossary in the O-TTPS.

The O-TTPS is technically equivalent to ISO/IEC 20243:2015. Throughout this document the term O-TTPS is used when referring to The Open Trusted Technology Provider Standard (O-TTPS) (ISO/IEC 20243:2015).

Note: The terms listed in the following sections are capitalized throughout this document.

1.3.1 Distributor

Distributors and Pass-Through Resellers distribute products, but do not modify the product or augment the physical composition of the product as they distribute it. Distributors and Pass-Through Resellers do have responsibility for mitigating risk to the physical and logical access to the product.

1.3.2 Evidence of Conformance

Evidence submitted to the assessor performing the assessment to demonstrate conformance to the O-TTPS Requirements within an Organization's declared Scope of Assessment.

1.3.3 Implementation Evidence

Artifacts that show the required process has been applied to the Selected Representative Products.

1.3.4 O-TTPS Requirements

All of the mandatory (i.e., Shall) requirements in the O-TTPS.

[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 and is available at: www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67394.

1.3.5 Organization

A technology provider being assessed for conformance to the O-TTPS Requirements (e.g., Original Equipment Manufacturer (OEM), Original Design Manufacturer (ODM), hardware and software component supplier, integrator, Value-Add Reseller (VAR), Distributor, or Pass-Through Reseller.

1.3.6 Pass-Through Reseller

Pass-Through Resellers distribute products, but do not modify the product or augment the physical composition of the product as they distribute it. Distributors and Pass-Through Resellers do have responsibility for mitigating risk to the physical and logical access to the product.

1.3.7 Process Evidence

The evidence/artifacts listed in this document as required to demonstrate that the Organization has the required processes/procedures defined.

Note: The Process Evidence shows they have defined/documented processes, the Implementation Evidence (see Section 1.3.3) demonstrates that the defined/documented processes/procedures have been implemented.

1.3.8 Scope of Assessment

A description by the Organization of the products, product lines, business units, and/or geographies, which optionally could encompass an entire organization.

1.3.9 Selected Representative Product

A set of products that is a representative sample of all the products from within the Scope of Assessment.