

# ISO/IEC 20243-1:2018-02 (E)

## Information technology - Open Trusted Technology Provider™ Standard (O-TTPS) - Mitigating maliciously tainted and counterfeit products - Part 1: Requirements and recommendations

---

| Contents |   | Page |
|----------|---|------|
| 1        | Introduction.....   | 1    |
| 1.1      | Objectives .....  | 1    |
| 1.2      | Overview.....   | 1    |
| 1.3      | Conformance.....  | 3    |
| 1.4      | Terminology .....   | 3    |
| 1.5      | Future Directions .....   | 4    |
| 2        | Business Context and Overview .....   | 5    |
| 2.1      | Business Environment Summary .....  | 5    |
| 2.1.1    | Operational Scenario .....  | 5    |
| 2.2      | Business Rationale.....   | 7    |
| 2.2.1    | Business Drivers.....   | 7    |
| 2.2.2    | Objectives and Benefits.....  | 8    |
| 2.3      | Recognizing the COTS ICT Context.....   | 9    |
| 2.4      | Overview.....   | 10   |
| 2.4.1    | O-TTPF Framework Overview .....   | 11   |
| 2.4.2    | Standard Overview .....   | 11   |
| 2.4.3    | Relationship with Other Standards.....  | 11   |
| 3        | O-TTPS – Tainted and Counterfeit Risks .....  | 13   |
| 4        | O-TTPS – Requirements for Addressing the Risks of Tainted and Counterfeit Products..... | 15   |
| 4.1      | Technology Development.....   | 16   |
| 4.1.1    | PD: Product Development/Engineering Method.....   | 16   |
| 4.1.1.1  | PD_DES: Software/Firmware/Hardware Design Process .....                                 | 16   |
| 4.1.1.2  | PD_CFM: Configuration Management.....   | 17   |
| 4.1.1.3  | PD_MPP: Well-defined Development/Engineering Method Process and Practices .....         | 17   |
| 4.1.1.4  | PD_QAT: Quality and Test Management.....  | 17   |
| 4.1.1.5  | PD_PSM: Product Sustainment Management .....  | 18   |
| 4.1.2    | SE: Secure Development/Engineering Method.....  | 18   |
| 4.1.2.1  | SE_TAM: Threat Analysis and Mitigation.....   | 18   |
| 4.1.2.2  | SE_RTP: Run-time Protection Techniques.....   | 19   |
| 4.1.2.3  | SE_VAR: Vulnerability Analysis and Response .....                                       | 19   |
| 4.1.2.4  | SE_PPR: Product Patching and Remediation .....  | 20   |
| 4.1.2.5  | SE_SEP: Secure Engineering Practices .....  | 20   |
| 4.1.2.6  | SE_MTL: Monitor and Assess the Impact of Changes in the Threat Landscape .....          | 20   |
| 4.2      | Supply Chain Security .....   | 21   |
| 4.2.1    | SC: Supply Chain Security.....  | 21   |
| 4.2.1.1  | SC_RSM: Risk Management.....  | 21   |

|          |   |    |
|----------|---|----|
| 4.2.1.2  | SC_PHS: Physical Security .....                               | 22 |
| 4.2.1.3  | SC_ACC: Access Controls .....                                 | 22 |
| 4.2.1.4  | SC_ESS: Employee and Supplier Security<br>and Integrity ..... | 23 |
| 4.2.1.5  | SC_BPS: Business Partner Security .....                       | 23 |
| 4.2.1.6  | SC_STR: Supply Chain Security Training .....                  | 24 |
| 4.2.1.7  | SC_ISS: Information Systems Security .....                    | 24 |
| 4.2.1.8  | SC_TTC: Trusted Technology Components.....                    | 24 |
| 4.2.1.9  | SC_STH: Secure Transmission and Handling .....                | 25 |
| 4.2.1.10 | SC_OSH: Open Source Handling .....                            | 25 |
| 4.2.1.11 | SC_CTM: Counterfeit Mitigation .....                          | 26 |
| 4.2.1.12 | SC_MAL: Malware Detection .....                               | 26 |

## List of Tables

|  |    |
|--|----|
| Table 1: O-TTPS Constituents and their Roles ..... | 6  |
| Table 2: Threat Mapping.....                       | 14 |

## List of Figures

|   |    |
|---|----|
| Figure 1: Constituents .....                                  | 6  |
| Figure 2: Product Life Cycle – Categories and Activities..... | 15 |