

# ISO/IEC 20153:2025-02 (E)

## Information technology - OASIS Common Security Advisory Framework (CSAF) v2.0 Specification

---

### Table of Contents

- [1 Introduction](#)
  - [1.1 IPR Policy](#)
  - [1.2 Terminology](#)
  - [1.3 Normative References](#)
  - [1.4 Informative References](#)
  - [1.5 Typographical Conventions](#)
- [2 Design Considerations](#)
  - [2.1 Construction Principles](#)
- [3 Schema Elements](#)
  - [3.1 Definitions](#)
    - [3.1.1 Acknowledgments Type](#)
      - [3.1.1.1 Acknowledgments Type - Names](#)
      - [3.1.1.2 Acknowledgments Type - Organization](#)
      - [3.1.1.3 Acknowledgments Type - Summary](#)
      - [3.1.1.4 Acknowledgments Type - URLs](#)
      - [3.1.1.5 Acknowledgments Type - Example](#)
    - [3.1.2 Branches Type](#)
      - [3.1.2.1 Branches Type - Branches](#)
      - [3.1.2.2 Branches Type - Category](#)
      - [3.1.2.3 Branches Type - Name](#)
        - [3.1.2.3.1 Branches Type - Name under Product Version](#)
        - [3.1.2.3.2 Branches Type - Name under Product Version Range](#)
      - [3.1.2.4 Branches Type - Product](#)
    - [3.1.3 Full Product Name Type](#)
      - [3.1.3.1 Full Product Name Type - Name](#)
      - [3.1.3.2 Full Product Name Type - Product ID](#)
      - [3.1.3.3 Full Product Name Type - Product Identification Helper](#)
        - [3.1.3.3.1 Full Product Name Type - Product Identification Helper - CPE](#)
        - [3.1.3.3.2 Full Product Name Type - Product Identification Helper - Hashes](#)
        - [3.1.3.3.3 Full Product Name Type - Product Identification Helper - Model Numbers](#)
        - [3.1.3.3.4 Full Product Name Type - Product Identification Helper - PURL](#)
        - [3.1.3.3.5 Full Product Name Type - Product Identification Helper - SBOM URLs](#)
        - [3.1.3.3.6 Full Product Name Type - Product Identification Helper - Serial Numbers](#)
        - [3.1.3.3.7 Full Product Name Type - Product Identification Helper - SKUs](#)
        - [3.1.3.3.8 Full Product Name Type - Product Identification Helper - Generic URIs](#)
    - [3.1.4 Language Type](#)
    - [3.1.5 Notes Type](#)
    - [3.1.6 Product Group ID Type](#)
    - [3.1.7 Product Groups Type](#)
    - [3.1.8 Product ID Type](#)
    - [3.1.9 Products Type](#)
    - [3.1.10 References Type](#)
    - [3.1.11 Version Type](#)
      - [3.1.11.1 Version Type - Integer versioning](#)
      - [3.1.11.2 Version Type - Semantic versioning](#)
  - [3.2 Properties](#)
    - [3.2.1 Document Property](#)
      - [3.2.1.1 Document Property - Acknowledgments](#)
      - [3.2.1.2 Document Property - Aggregate Severity](#)
      - [3.2.1.3 Document Property - Category](#)
      - [3.2.1.4 Document Property - CSAF Version](#)
      - [3.2.1.5 Document Property - Distribution](#)
        - [3.2.1.5.1 Document Property - Distribution - Text](#)
        - [3.2.1.5.2 Document Property - Distribution - TLP](#)
      - [3.2.1.6 Document Property - Language](#)

- [3.2.1.7 Document Property - Notes](#)
- [3.2.1.8 Document Property - Publisher](#)
  - [3.2.1.8.1 Document Property - Publisher - Category](#)
  - [3.2.1.8.2 Document Property - Publisher - Contact Details](#)
  - [3.2.1.8.3 Document Property - Publisher - Issuing Authority](#)
  - [3.2.1.8.4 Document Property - Publisher - Name](#)
  - [3.2.1.8.5 Document Property - Publisher - Namespace](#)
- [3.2.1.9 Document Property - References](#)
- [3.2.1.10 Document Property - Source Language](#)
- [3.2.1.11 Document Property - Title](#)
- [3.2.1.12 Document Property - Tracking](#)
  - [3.2.1.12.1 Document Property - Tracking - Aliases](#)
  - [3.2.1.12.2 Document Property - Tracking - Current Release Date](#)
  - [3.2.1.12.3 Document Property - Tracking - Generator](#)
  - [3.2.1.12.4 Document Property - Tracking - ID](#)
  - [3.2.1.12.5 Document Property - Tracking - Initial Release Date](#)
  - [3.2.1.12.6 Document Property - Tracking - Revision History](#)
  - [3.2.1.12.7 Document Property - Tracking - Status](#)
  - [3.2.1.12.8 Document Property - Tracking - Version](#)
- [3.2.2 Product Tree Property](#)
  - [3.2.2.1 Product Tree Property - Branches](#)
  - [3.2.2.2 Product Tree Property - Full Product Names](#)
  - [3.2.2.3 Product Tree Property - Product Groups](#)
  - [3.2.2.4 Product Tree Property - Relationships](#)
- [3.2.3 Vulnerabilities Property](#)
  - [3.2.3.1 Vulnerabilities Property - Acknowledgments](#)
  - [3.2.3.2 Vulnerabilities Property - CVE](#)
  - [3.2.3.3 Vulnerabilities Property - CWE](#)
  - [3.2.3.4 Vulnerabilities Property - Discovery Date](#)
  - [3.2.3.5 Vulnerabilities Property - Flags](#)
  - [3.2.3.6 Vulnerabilities Property - IDs](#)
  - [3.2.3.7 Vulnerabilities Property - Involvements](#)
  - [3.2.3.8 Vulnerabilities Property - Notes](#)
  - [3.2.3.9 Vulnerabilities Property - Product Status](#)
  - [3.2.3.10 Vulnerabilities Property - References](#)
  - [3.2.3.11 Vulnerabilities Property - Release Date](#)
  - [3.2.3.12 Vulnerabilities Property - Remediations](#)
    - [3.2.3.12.1 Vulnerabilities Property - Remediations - Category](#)
    - [3.2.3.12.2 Vulnerabilities Property - Remediations - Date](#)
    - [3.2.3.12.3 Vulnerabilities Property - Remediations - Details](#)
    - [3.2.3.12.4 Vulnerabilities Property - Remediations - Entitlements](#)
    - [3.2.3.12.5 Vulnerabilities Property - Remediations - Group IDs](#)
    - [3.2.3.12.6 Vulnerabilities Property - Remediations - Product IDs](#)
    - [3.2.3.12.7 Vulnerabilities Property - Remediations - Restart Required](#)
    - [3.2.3.12.8 Vulnerabilities Property - Remediations - URL](#)
  - [3.2.3.13 Vulnerabilities Property - Scores](#)
  - [3.2.3.14 Vulnerabilities Property - Threats](#)
  - [3.2.3.15 Vulnerabilities Property - Title](#)

[4.1 Profile 1: CSAF Base](#)

[4.2 Profile 2: Security incident response](#)

[4.3 Profile 3: Informational Advisory](#)

[4.4 Profile 4: Security Advisory](#)

[4.5 Profile 5: VEX](#)

## [5 Additional Conventions](#)

[5.1 Filename](#)

[5.2 Separation in Data Stream](#)

## 6 Tests

### 6.1 Mandatory Tests

- [6.1.1 Missing Definition of Product ID](#)
- [6.1.2 Multiple Definition of Product ID](#)
- [6.1.3 Circular Definition of Product ID](#)
- [6.1.4 Missing Definition of Product Group ID](#)
- [6.1.5 Multiple Definition of Product Group ID](#)
- [6.1.6 Contradicting Product Status](#)
- [6.1.7 Multiple Scores with same Version per Product](#)
- [6.1.8 Invalid CVSS](#)
- [6.1.9 Invalid CVSS computation](#)
- [6.1.10 Inconsistent CVSS](#)
- [6.1.11 CWE](#)
- [6.1.12 Language](#)
- [6.1.13 PURL](#)
- [6.1.14 Sorted Revision History](#)
- [6.1.15 Translator](#)
- [6.1.16 Latest Document Version](#)
- [6.1.17 Document Status Draft](#)
- [6.1.18 Released Revision History](#)
- [6.1.19 Revision History Entries for Pre-release Versions](#)
- [6.1.20 Non-draft Document Version](#)
- [6.1.21 Missing Item in Revision History](#)
- [6.1.22 Multiple Definition in Revision History](#)
- [6.1.23 Multiple Use of Same CVE](#)
- [6.1.24 Multiple Definition in Involvements](#)
- [6.1.25 Multiple Use of Same Hash Algorithm](#)
- [6.1.26 Prohibited Document Category Name](#)
- [6.1.27 Profile Tests](#)
  - [6.1.27.1 Document Notes](#)
  - [6.1.27.2 Document References](#)
  - [6.1.27.3 Vulnerabilities](#)
  - [6.1.27.4 Product Tree](#)
  - [6.1.27.5 Vulnerability Notes](#)
  - [6.1.27.6 Product Status](#)
  - [6.1.27.7 VEX Product Status](#)
  - [6.1.27.8 Vulnerability ID](#)
  - [6.1.27.9 Impact Statement](#)
  - [6.1.27.10 Action Statement](#)
  - [6.1.27.11 Vulnerabilities](#)
- [6.1.28 Translation](#)
- [6.1.29 Remediation without Product Reference](#)
- [6.1.30 Mixed Integer and Semantic Versioning](#)
- [6.1.31 Version Range in Product Version](#)
- [6.1.32 Flag without Product Reference](#)
- [6.1.33 Multiple Flags with VEX Justification Codes per Product](#)

### 6.2 Optional Tests

- [6.2.1 Unused Definition of Product ID](#)
- [6.2.2 Missing Remediation](#)
- [6.2.3 Missing Score](#)
- [6.2.4 Build Metadata in Revision History](#)
- [6.2.5 Older Initial Release Date than Revision History](#)
- [6.2.6 Older Current Release Date than Revision History](#)
- [6.2.7 Missing Date in Involvements](#)
- [6.2.8 Use of MD5 as the only Hash Algorithm](#)
- [6.2.9 Use of SHA-1 as the only Hash Algorithm](#)
- [6.2.10 Missing TLP label](#)
- [6.2.11 Missing Canonical URL](#)

- [6.2.12 Missing Document Language](#)
  - [6.2.13 Sorting](#)
  - [6.2.14 Use of Private Language](#)
  - [6.2.15 Use of Default Language](#)
  - [6.2.16 Missing Product Identification Helper](#)
  - [6.2.17 CVE in field IDs](#)
  - [6.2.18 Product Version Range without vers](#)
  - [6.2.19 CVSS for Fixed Products](#)
  - [6.2.20 Additional Properties](#)
- [6.3 Informative Test](#)
  - [6.3.1 Use of CVSS v2 as the only Scoring System](#)
  - [6.3.2 Use of CVSS v3.0](#)
  - [6.3.3 Missing CVE](#)
  - [6.3.4 Missing CWE](#)
  - [6.3.5 Use of Short Hash](#)
  - [6.3.6 Use of non-self referencing URLs Failing to Resolve](#)
  - [6.3.7 Use of self referencing URLs Failing to Resolve](#)
  - [6.3.8 Spell check](#)
  - [6.3.9 Branch Categories](#)
  - [6.3.10 Usage of Product Version Range](#)
  - [6.3.11 Usage of V as Version Indicator](#)
- [7 Distributing CSAF documents](#)
  - [7.1 Requirements](#)
    - [7.1.1 Requirement 1: Valid CSAF document](#)
    - [7.1.2 Requirement 2: Filename](#)
    - [7.1.3 Requirement 3: TLS](#)
    - [7.1.4 Requirement 4: TLP:WHITE](#)
    - [7.1.5 Requirement 5: TLP:AMBER and TLP:RED](#)
    - [7.1.6 Requirement 6: No Redirects](#)
    - [7.1.7 Requirement 7: provider-metadata.json](#)
    - [7.1.8 Requirement 8: security.txt](#)
    - [7.1.9 Requirement 9: Well-known URL for provider-metadata.json](#)
    - [7.1.10 Requirement 10: DNS path](#)
    - [7.1.11 Requirement 11: One folder per year](#)
    - [7.1.12 Requirement 12: index.txt](#)
    - [7.1.13 Requirement 13: changes.csv](#)
    - [7.1.14 Requirement 14: Directory listings](#)
    - [7.1.15 Requirement 15: ROLIE feed](#)
    - [7.1.16 Requirement 16: ROLIE service document](#)
    - [7.1.17 Requirement 17: ROLIE category document](#)
    - [7.1.18 Requirement 18: Integrity](#)
    - [7.1.19 Requirement 19: Signatures](#)
    - [7.1.20 Requirement 20: Public OpenPGP Key](#)
    - [7.1.21 Requirement 21: List of CSAF providers](#)
    - [7.1.22 Requirement 22: Two disjoint issuing parties](#)
    - [7.1.23 Requirement 23: Mirror](#)
  - [7.2 Roles](#)
    - [7.2.1 Role: CSAF publisher](#)
    - [7.2.2 Role: CSAF provider](#)
    - [7.2.3 Role: CSAF trusted provider](#)
    - [7.2.4 Role: CSAF lister](#)
    - [7.2.5 Role: CSAF aggregator](#)
  - [7.3 Retrieving rules](#)
    - [7.3.1 Finding provider-metadata.json](#)
    - [7.3.2 Retrieving CSAF documents](#)
- [8 Safety, Security, and Data Protection Considerations](#)
- [9 Conformance](#)
  - [9.1 Conformance Targets](#)

- [9.1.1 Conformance Clause 1: CSAF document](#)
- [9.1.2 Conformance Clause 2: CSAF producer](#)
- [9.1.3 Conformance Clause 3: CSAF direct producer](#)
- [9.1.4 Conformance Clause 4: CSAF converter](#)
- [9.1.5 Conformance Clause 5: CVRF CSAF converter](#)
- [9.1.6 Conformance Clause 6: CSAF content management system](#)
- [9.1.7 Conformance Clause 7: CSAF post-processor](#)
- [9.1.8 Conformance Clause 8: CSAF modifier](#)
- [9.1.9 Conformance Clause 9: CSAF translator](#)
- [9.1.10 Conformance Clause 10: CSAF consumer](#)
- [9.1.11 Conformance Clause 11: CSAF viewer](#)
- [9.1.12 Conformance Clause 12: CSAF management system](#)
- [9.1.13 Conformance Clause 13: CSAF asset matching system](#)
- [9.1.14 Conformance Clause 14: CSAF basic validator](#)
- [9.1.15 Conformance Clause 15: CSAF extended validator](#)
- [9.1.16 Conformance Clause 16: CSAF full validator](#)
- [9.1.17 Conformance Clause 17: CSAF SBOM matching system](#)

[Appendix A. Acknowledgments](#)

[Appendix B. Revision History](#)

[Appendix C. Guidance on the Size of CSAF Documents](#)

- [C.1 File size](#)
- [C.2 Array length](#)
- [C.3 String length](#)
- [C.4 URI length](#)
- [C.5 Enum](#)
- [C.6 Date](#)