INTERNATIONAL STANDARD

ISO/IEC
15292

First edition
2001-12-15

Information technology — Security techniques — Protection Profile registration procedures

Technologies de l'information — Techniques de sécurité — Procédures d'enregistrement du profil de protection

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 15292:2001
https://standards.iteh.ai/catalog/standards/sist/7fbd5725-577d-467f-8cc9-
37efc431e998/iso-iec-15292-2001

Contents

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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 15292 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Security techniques*.

Annexes A and B of this International Standard are for information only.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 15292:2001
https://standards.iteh.ai/catalog/standards/sist/7fbd5725-577d-467f-8cc9-
37efc431e998/iso-iec-15292-2001

Information technology — Security techniques — Protection Profile registration procedures

1 Scope

This International Standard defines the procedures to be applied by the JTC 1 Registration Authority appointed by the ISO and IEC councils to maintain a register of Protection Profiles and packages for the purposes of IT security evaluation. These Protection Profiles and packages are specified in accordance with criteria given in ISO/IEC 15408.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this International Standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this International Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards.

ISO 15408-1, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO 15408-2, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functionality requirements*

ISO 15408-3, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security assurance requirements*

Procedures for the technical work of ISO/IEC JTC 1

ISO/IEC/ITU ITSIG Guide for the use of IT in the development and delivery of standards

3 Terms and definitions

For the purposes of this International Standard, the following terms and definitions apply.

3.1
applicant
an entity (organisation, individual etc.) which requests the assignment of a register entry and entry label

3.2
certificate
a declaration by an independent authority operating in accordance with ISO Guide 58, Calibration and testing laboratory accreditation systems - General requirements for operation and recognition, confirming that an evaluation pass statement is valid

3.3
entry label
the naming information that identifies a registered PP or package uniquely

3.4
evaluation pass statement
a statement issued by an organisation that performs evaluations against ISO/IEC 15408 confirming that a PP has successfully passed assessment against the evaluation criteria given in clause 4 of Part 3 of that International Standard

3.5
JTC 1 Registration Authority
an organisation appointed by the ISO and IEC councils to register objects in accordance with a JTC 1 procedural Standard

3.6
package
a reusable set of either functional or assurance components combined together to satisfy a set of identified security objectives (from ISO/IEC 15408-1)

3.7
Protection Profile
an implementation-independent set of security requirements for a category of IT products or systems that meet specific consumer needs (adapted from ISO/IEC 15408-1)

3.8
register
a set of files (electronic, or a combination of electronic and paper) containing entry labels and their associated definitions and related information

3.9
register entry
the information within a register relating to a specific PP or package

3.10
registration
the process of assigning a register entry

3.11
Security Target
a set of security requirements and specifications to be used as the basis for evaluation of an identified IT product or system (adapted from ISO/IEC 15408-1)

3.12
sponsor
an entity (organisation, individual etc.) responsible for the content of a register entry

4   Abbreviations

ITTF   Information Technology Task Force (of ISO/IEC)
PP   Protection Profile
RA   Registration Authority
SC   JTC 1 Subcommittee
ST   Security Target

5   Technical Specifications

5.1   Entry label

Every PP or package registered in accordance with this International Standard shall have an entry label assigned by the JTC 1 RA that uniquely identifies that PP or package within the register. The entry label shall be made up of the following elements, separated by dashes:

-        Entry Type
-        Registration Year
-        Registration Number.

The Entry Type shall be PP for a protection profile, AP for an assurance package or FP for a functional package.

The Registration Year shall be the four digit representation of the year when the entry was registered.

The Registration Number shall be a four digit sequentially assigned identification number, starting each year from 0001.

EXAMPLE   PP-2001-0001.

5.2   Technical definition (within a register entry)

5.2.1   PPs

Every application for registration of a PP submitted for registration in accordance with this International Standard shall include a technical definition of the PP in question. This technical definition shall conform to the content requirements for PPs contained within Annex B to ISO/IEC 15408-1 and shall conform to the structural outline portrayed in Figure B.1 of ISO/IEC 15408-1.

5.2.2   Packages

Every application for registration of a functional or assurance package submitted for registration in accordance with this International Standard shall include a technical definition of the package. This definition shall contain:

-        a package overview that summarises the package in narrative form
-        a specification of a set of either functional or assurance components.

The package overview should be sufficiently detailed for a potential user of the package to determine whether the package is of interest. It should be understandable without reference to the component specifications.

3

Components for functional packages shall be selected from ISO/IEC 15408-2 or shall be constructed and specified in accordance with the specification requirements for functional components given within clause 2 of ISO/IEC 15408-2.

Components for assurance packages shall be selected from ISO/IEC 15408-3 or shall be constructed and specified in accordance with the specification requirements for assurance components given within subclause 2.1 of ISO/IEC 15408-3.

The technical definition of a package may contain other descriptive information that might be relevant to the author of a PP or ST wishing to use or reference the package. This information shall be presented in the form of one or more named PP or ST sections as defined within Annexes B and C of ISO/IEC 15408-1. The information should be suitable for direct incorporation within PPs or STs that make use of the package.

6 The JTC 1 Registration Authority for PPs and packages

6.1 Appointment

The JTC 1 RA for PPs and packages shall be appointed by the ISO and IEC councils in accordance with the procedure for the appointment of JTC 1 Registration Authorities defined in the JTC 1 Directives.

6.2 Qualifications

Any organisation seeking appointment as the JTC 1 RA for PPs and packages shall demonstrate that it meets the qualifications required of JTC 1 RAs as defined in the JTC 1 Directives, with the following amendments:

- it shall confirm its agreement to function as an RA for a minimum of 5 years;

- it shall confirm that it has sufficient equipment resources and communication facilities to operate an Internet web site in support of this International Standard;

- it shall confirm that on termination of its appointment, it will transfer its register and all supporting documentation at no cost to another organisation designated by the ISO and IEC councils.

6.3 Contract

The JTC 1 RA for PPs and packages shall operate under contract with the ITTF. Upon twelve-months notice, either the RA or the ITTF may terminate the contract.

NOTE   The contract has no fixed time limit. Although the organisation appointed as the JTC1 RA will have committed to function as the RA for a minimum of 5 years from the date of first appointment, circumstances can change. This subclause permits the RA to resign from its duties at any time, including before the 5 years is complete, provided that the twelve months notice is given.

6.4 Duties

The JTC 1 RA for PPs and packages shall:

- receive applications for the registration of PPs and packages;

- review applications for the registration of PPs and packages;

- assign unique entry labels to PPs and packages added to the register;

- inform applicants for registration of the results of their applications;

- inform sponsors of the results of actions relating to their register entries;

- maintain an accurate register;

- make public access to all register entries available at no cost via the world wide web and provide printed details of register entries on demand, in return for payment of a fee if required;

- publish details of its fee structure, if it operates on such terms;

- handle all aspects of the registration process in accordance with good business practice;

- provide an annual summary report on its activities to JTC 1, ITTF and the SC responsible for this International Standard;

- adhere to the procedure for appeals contained within clause 15 of this International Standard;

- maintain a copy of the register in the English language;

- handle all correspondence relating to the register or register access in the English language;

- produce guidance, practice and tutorial web pages and documents where applicable;

- indicate (e.g. on web pages and stationery) that it has been designated a JTC 1 RA in accordance with this International Standard by ISO/IEC.

7   Criteria for eligibility of applicants for registration

Any organisation or individual may submit an application for registration of a PP or package to the JTC 1 RA for PPs and packages.

8   Information to be included within an application for registration

An application for registration of a PP or package shall include:

- the name and contact details of the applicant. The contact details shall include both a postal or E-mail address and a telephone or facsimile number. If the applicant is an organisation, the contact details shall identify the name and title of a contact person within the organisation and provide sufficient information for contact to be made with that person;

- the type of object submitted for registration. This shall be a PP, functional package or assurance package;

- a statement as to whether the PP or package is submitted for registration as a new entry or replacement entry. If the PP or package is submitted as a replacement entry, the entry labels of the existing register entries to be replaced shall be identified. The application shall include a statement

from the sponsors of those entries confirming that if the replacement entry is accepted, they will agree to the linking of their existing entries as replaced by this entry;

- a statement as to whether the PP or package is submitted for registration as draft or complete;

- the technical definition of the new PP or package, structured in accordance with subclause 5.2 of this International Standard;

- a statement identifying the natural language in which the technical definition of the PP or package is written, if not English;

- an executive summary that summarises the PP or package in narrative form;

- a declaration that the applicant will sponsor the register entry until its first routine review;

- a declaration that the technical definition of the PP or package submitted for registration does not contain secret, proprietary or non-publishable information;

- a declaration that the technical definition of the PP or package submitted for registration meets the requirements of subclause 5.2 of this International Standard.

- any initial fee required by the RA for consideration of the application;

An application for registration of a PP may also include:

- an evaluation pass statement or certificate for the PP in question, together with the name and contact details of the organisation that issued that statement or certificate.

NOTE   Most elements within an application for registration provide information about the status and attributes of the proposed entry. It is the technical definition that actually specifies the PP or package that is to be registered.

Application for registration shall be made in the English language and, with the exception of the technical definition of the PP or package, all information supplied shall be in English. The technical definition of the PP or package may be written in any natural language. The executive summary shall be identical in content to the PP or package overview within the technical definition, but shall always be in the English language.

The technical definition of a PP or package submitted for registration shall contain all the mandatory structural elements required by subclause 5.2 of this International Standard, and these structural elements shall be readily identifiable within the text of the definition. If an entry is designated as draft, elements may be marked as to be defined later, or may be marked as inconsistent or incomplete.

The technical definition shall not reference other PP or package specifications for definition purposes, whether these specifications are registered or otherwise.

Versions of the technical definition in several natural languages may be supplied. However, one version shall be identified as the official version for the register entry and all other versions as informative translations.

An electronic copy of the technical definition shall be supplied with the application. This electronic copy shall use a file format and transport mechanism recommended for the exchange of electronic documents within the ISO/IEC/ITU Guide for the use of IT in the development and delivery of standards.

9   Steps involved in review and response to an application

9.1   Initial processing

All applications for registration of PPs or packages in accordance with this International Standard shall be subjected to initial processing by the RA.

This process shall check that all required elements of the application are present, and in the opinion of the RA, adequate for further processing.

The RA shall either reject the application or assign the PP or package an entry label and enter the PP or package into the register with a status of "in validation". The applicant shall be advised accordingly. If the application is rejected, the RA shall identify within its response the reasons for its rejection.

This process shall be completed within 14 days of receipt of the application.

9.2   Validation

The RA shall perform a structural check of the technical definition provided within the application for registration.   If the RA identifies missing sections, or information presented in a manner which is incompatible with the current version of this International Standard or of ISO/IEC 15408, including relevant technical corrigenda or amendments published by the ITTF, the RA shall refer the issue or issues to the applicant for clarification or rectification. If the applicant cannot resolve omissions or inconsistencies within 14 days of receipt of notification of the issue, the PP or package shall fail validation.

If an evaluation pass statement or certificate is supplied, the RA shall contact the organisation that issued the statement or certificate and provide them with a copy of the application. The evaluating or certifying organisation shall be requested to confirm within one month that the technical definition of the PP as evaluated is identical to that as submitted for registration, and that the PP was awarded a pass statement. If the organisation cannot be contacted, does not reply, or does not offer the requested confirmation, the RA shall declare the statement or certificate not acceptable and advise the applicant accordingly.

If the application for registration identifies one or more existing register entries that are to be replaced, the RA shall contact the organisations that currently sponsor those entries and provide them with a copy of the application and their statement agreeing to the linking of their entries as replaced. The sponsoring organisations shall be requested to confirm within one month the validity of these statements. If any organisation cannot be contacted, does not reply, or does not offer the requested confirmation, the RA shall declare the replacement linkage not accepted and advise the applicant accordingly.

The RA shall complete this validation, including any referrals that are necessary, within 3 months of receipt of the application. If the applicant has been unable to resolve an issue, the register entry shall then be given a status of "failed validation".   Otherwise the status shall become either "registered", or in the case of a complete PP where an acceptable evaluation pass statement or certificate was supplied, "evaluated" or "certified" as appropriate. The routine review date shall be set to 36 months from the date of initial entry onto the register. The applicant shall be recorded within the register entry as the original applicant for registration and as the current sponsor of the entry.

NOTE Validation by the RA is restricted to the structural and consistency checks defined above and does not include evaluation of the technical definition using ISO/IEC 15408. The RA will not perform any technical check of the PP or package definition and it is therefore possible that an incomplete or inconsistent PP or package definition will be accepted for registration. Only where an entry has "evaluated" or "certified" status is any assertion