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

Reference number
ISO/IEC 15292:2001(E)

© ISO/IEC 2001

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

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.

© ISO/IEC 2001

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

© ISO/IEC 2001 – All rights reserved

Not for Resale

Contents

1 Scope ... 1

2 Normative references ... 1

3 Terms and definitions ... 1

4 Abbreviations ... 3

5 Technical Specifications ... 3
5.1 Entry label ... 3
5.2 Technical definition (within a register entry) ... 3

6 The JTC 1 Registration Authority for PPs and packages ... 4
6.1 Appointment ... 4
6.2 Qualifications ... 4
6.3 Contract ... 4
6.4 Duties ... 4

7 Criteria for eligibility of applicants for registration ... 5

8 Information to be included within an application for registration ... 5

9 Steps involved in review and response to an application ... 7
9.1 Initial processing ... 7
9.2 Validation ... 7

10 Criteria for rejection of applications for registration ... 8

11 Operation of the register ... 8
11.1 Notification of obsolescent entries ... 8
11.2 Update of draft technical specifications ... 8
11.3 Routine review of entries ... 8
11.4 Defect notification ... 9
11.5 Other requests for update of entries ... 9
11.6 Deletion of register entries ... 10

12 Maintenance of the register ... 10

13 Confidentiality of information held within the register ... 10

14 Publication of the register ... 10

15 Appeals procedure ... 12

Annex A (informative) Benefits of registration ... 13

Annex B (informative) Lifecycle of a register entry ... 14

--`,,```,,,,````-`-`,,`,,`,`,,`---

© ISO/IEC 2001 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

© ISO/IEC 2001 – All rights reserved

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

© ISO/IEC 2001 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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

© ISO/IEC 2001 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

© ISO/IEC 2001 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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;

© ISO/IEC 2001 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

- 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

© ISO/IEC 2001 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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.

© ISO/IEC 2001 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

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

© ISO/IEC 2001 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

made in the register concerning the technical accuracy of the technical definition.

10 Criteria for rejection of applications for registration

An application for registration of a PP or package shall be rejected if:

- the applicant fails to pay any fee required by the RA;
- required elements of the application are missing;
- the application contains missing or incomplete information (except where expressly permitted by this International Standard);
- the application contains information designated secret, proprietary or non-publishable;
- the application contains incomprehensible information;
- the technical definition of the PP or package to be registered is not in accordance with the requirements of this International Standard.

11 Operation of the register

11.1 Notification of obsolescent entries

The RA may be advised at any time by the sponsor of a register entry with “registered”, “evaluated” or “certified” status that the entry in question is considered unsuitable for future use on grounds of obsolescence. The register entry status shall be updated to “obsolescent”, and the routine review date shall be set to 18 months from the date of receipt of the advice.

11.2 Update of draft technical specifications

The sponsor of a draft register entry may request the RA at any time to replace all or part of the registered technical definition or executive summary with a revised specification. The RA shall perform a structural check of the revised technical definition. 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. Otherwise the entry shall be updated as requested within 14 days of receipt of the request.

The RA may charge a fee for such updates to draft entries.

11.3 Routine review of entries

One month prior to the routine review date of entries with a status of “evaluated” or “certified”, the RA shall contact the organisation that issued the evaluation pass statement or certificate, providing a copy of the current register entry, including any defect reports and defect resolution notes. The evaluating or certifying organisation shall be requested to confirm within one month that the pass statement or certificate is still valid. If the organisation cannot be contacted, does not reply, or does not offer the requested confirmation,

© ISO/IEC 2001 – All rights reserved

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

the RA shall downgrade the status of the entry to “registered”, and advise the sponsor of the entry accordingly.

One month prior to the routine review date of all entries with a status of “registered”, “evaluated” or “certified”, the RA shall contact the sponsor of the entry in order to check that the sponsor wishes to continue registration. The RA may require the payment of a further fee for continuing registration. If the sponsor of the entry advises that they do not wish to continue registration, or does not reply within one month of the revalidation request, or does not pay any required fee, the status of the register entry shall become “obsolescent”.

The routine review date shall be updated to be 18 months from the date of review for entries now marked “obsolescent” and to be 36 months from the date of review in all other cases.

On the routine review date for entries with the status of “obsolescent”, their status shall become “retired”.

11.4 Defect notification

The RA may be advised at any time by any person of a claimed error, defect, inconsistency or ambiguity within a register entry. Upon receipt of such a report, the RA shall advise the sponsor of the register entry of the claimed defect.

In the case of draft entries, the sponsor need not respond to the defect report, but may submit an updated technical definition of the PP or package to resolve the issue.

In the case of complete entries, if within one month the person reporting the claimed defect withdraws the notification, the register entry shall remain unchanged. Otherwise, the sponsor of the entry shall within that time period provide a defect resolution note describing the problem and providing a response. This may be to record that, in the opinion of the entry sponsor, no defect exists. The RA shall append the defect report and its resolution note to the register entry. The RA shall also send a copy of the resolution note to the person who reported the defect.

Defect reports and defect resolution notes shall be submitted to the RA in the English language, but may include references to and extracts from the technical definition in the language used within that definition.

NOTE The sponsor of the register entry is encouraged to contact the person reporting the defect in order to reach a mutually agreeable response, but is not required to do so. There will be some types of defects that cannot be solved by means of a defect resolution note. In such cases, a replacement entry will need to be registered and the existing entry marked as obsolescent.

Where a defect resolution note is required, but is not supplied by the sponsor within the required time, the status of the register entry shall become “obsolescent”. The defect report shall be appended to the register entry and the date of next routine review set to 18 months from the date of the change of status.

If ISO/IEC 15408 is amended, or found to be defective, then register entries can become inconsistent or defective when compared against the revised criteria. Such defects shall be recorded if reported.

11.5 Other requests for update of entries

The RA may be advised at any time by the sponsor of a register entry of changed contact details for the sponsor. Within one week of receipt, the RA shall update the register entry accordingly.

At any time the sponsor of a register entry may request that sponsorship of the entry is transferred to another person or organisation. Such requests shall include a statement from the proposed new sponsor

© ISO/IEC 2001 – All rights reserved

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

accepting the transfer of sponsorship and providing its contact details. Within one week of receipt, the RA shall update the register entry accordingly, advising both new and old sponsors that the change has been made.

The RA may receive at any time from the sponsor of a complete PP register entry with “registered” status an evaluation pass statement or certificate for the entry in question. Upon receipt, the evaluating or certifying organisation shall be requested to confirm within one month that the PP was awarded a pass statement, and that the technical definition of the PP as evaluated is identical to that registered. 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 that the status of “registered” remains unchanged. Otherwise the status of the entry shall be updated to “evaluated” or “certified”, as appropriate.

The RA may be advised at any time by the organisation that issued an evaluation pass statement or certificate referenced in a register entry with “evaluated” or “certified” status that the statement or certificate in question has been withdrawn. Upon receipt of such notification, the status of the register entry shall be downgraded to “registered”.

None of the register entry changes permitted by this subclause shall change the date of next routine review for the entry.

11.6 Deletion of register entries

Register entries once allocated an entry label shall never be deleted from the register.

NOTE Entries that are no longer in active use can be distinguished by their “retired” status.

12 Maintenance of the register

The RA shall take appropriate measures to ensure that accuracy of the information within the register is maintained, information within the register is publicly accessible without unreasonable delay, and that adequate backup and recovery measures exist to protect the register.

These measures shall be specified in the contract between the RA and ITTF.

13 Confidentiality of information held within the register

Register entries shall not contain secret, proprietary or non-publishable material. All information within all register entries shall be made publicly available by the RA.

14 Publication of the register

The JTC 1 RA appointed under the terms of this International Standard shall maintain a register of all PPs and packages that it has accepted for registration. The register shall be maintained and published in the English language. Informative translations of the register or individual register entries may also, if the RA wishes, be provided in other languages.

The register entry for each PP or package shall contain at least the following information:

- The entry label for the entry;

© ISO/IEC 2001 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

- The type of object registered, either “PP”, “functional package” or “assurance package”;
- Whether the entry is a new or replacement entry;
- Whether the entry is draft or complete;
- The status of the entry, one of “in validation”, “failed validation”, “registered”, “evaluated”, “certified”, “obsolescent”, or “retired”;
- The date of original acceptance of the entry;
- The date of the last change to the entry;
- The date for the next routine review of the entry;
- The name and contact details of the current sponsor of the entry;
- The name and contact details of the original applicant for registration;
- Where the status of the entry is “evaluated” or “certified”, the name and contact details of the organisation that issued the evaluation pass statement or certificate;
- The executive summary of the PP or package;
- Identification of the language in which the technical definition of the PP or package is written, where this is not English;
- The technical definition of the PP or package, structured in accordance with subclause 5.2 of this International Standard;
- In the case of complete entries, any applicable defect reports and defect resolution notes;
- The version of ISO/IEC 15408 against which the entry was validated by the RA, including any relevant technical corrigenda or amendments published by the ITTF that were taken into account;
- The entry labels of any entries replaced by the entry;
- The entry label of any entry replacing this entry.

NOTE Most fields within a register entry provide information about the status and attributes of the entry. It is the technical definition that actually specifies the PP or package in question.

Although the register is maintained and published in English, technical definitions may be written in languages other than English. The executive summary will always provide an overview of the PP or package in English. Defect reports and defect resolution notes shall be published in English but may include references to and extracts from the technical definition in the language used within that definition.

The RA shall make access available at no cost to all the information identified above for all register entries, via the world wide web.

Upon request, and upon payment of a fee if applicable, the RA shall provide printed details of one or more register entries containing all the information identified above.

© ISO/IEC 2001 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

Upon request, and upon payment of a fee if applicable, the RA shall provide a printed copy of the complete register.

Register extracts and copies of the complete register shall display a prominent notice that the RA is not liable for the content of register entries, which are the responsibility of entry sponsors. The notice shall state that validation of register entries by the RA is restricted to structural and consistency checks and does not include evaluation of the technical definition using ISO/IEC 15408. Only where an entry has “evaluated” or “certified” status is an assertion made in the register concerning the technical accuracy of the technical definition.

15 Appeals procedure

In the event of a dispute between an applicant for registration or the sponsor of a register entry and the RA, the applicant or sponsor shall contact the chief executive of the RA in writing, setting out the grounds for disagreement and the action requested of the RA.

The chief executive of the RA shall consider the issue in question, and within one month issue a decision in writing to the complainant and to the operational staff of the RA.

If the complainant is not satisfied by the decision of the chief executive, the complainant shall within one month appeal formally to the chief executive in writing, setting out the grounds for non-acceptance of the decision.

The chief executive shall consider the grounds for appeal, and within one month confirm or revise his or her previous decision in writing.

If the complainant is not satisfied by the appeal decision of the chief executive, the complainant shall within one month write to the secretariat of the JTC 1 subcommittee responsible for this International Standard, setting out the grounds of the dispute, the decision of the chief executive of the RA and the grounds for non-acceptance of that decision.

The secretariat shall request the issue to be considered by the SC responsible for this International Standard. Upon such a request, within 15 months the relevant SC shall by resolution provide a decision to the issue in question, which shall thenceforth be binding upon both the complainant and the RA.

© ISO/IEC 2001 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex A
(informative)

Benefits of registration

The benefits of registration of PPs and packages are:

- as a shorthand way to publicise common security requirements, to assist users to compare the security claims of competing products or systems;

- as a way that industry sector or product vendor associations can specify minimum standards for security functionality and assurance, as a public guide to prospective product manufacturers developing new commercial products;

- as a public domain basis for purchasers to specify security requirements for incorporation within multiple acquisition specifications;

- where a PP has been evaluated, developers of Targets of Evaluation (TOEs) incorporating that PP will benefit by a reduction in cost, risk and complexity of evaluation, since the PP portion of the work will not need to be repeated.

Entries which are designated as draft can be used to stimulate discussion of desirable security features, to publicise work in progress, or to indicate areas of specification of common requirements where technical problems exist. As development proceeds and problems are identified and resolved, the entry sponsor can update the entry at any time to reflect progress.

Entries which are designated complete will not change; any errors that are found are handled by appending defect resolution notes. Other parties can therefore use such entries with the confidence that the specification will remain stable. Complete PPs that have evaluated or certified status give confidence in the correctness of the PP specification from assurance that a formal evaluation of the PP has been successfully completed, and in the case of certified PPs, that an independent third party unconnected with the evaluation process has then validated the evaluation. In the event that a major flaw is subsequently found in an entry, there is a guaranteed transition period of obsolescence before the entry is fully retired from active use.

© ISO/IEC 2001 – All rights reserved

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex B
(informative)

Lifecycle of a register entry

When a request for registration is received from an applicant, the RA performs an initial check that all the required information (and any initial fee) is present. Provided that this is the case, the PP or package is assigned a unique registration identifier (entry label), and is added to the register with an initial status of “in validation”.

The RA then contacts other parties involved in the registration process, such as the sponsors of related entries or any evaluator or certifier. The RA also makes a structural check of the PP or package to ensure that there are no obvious omissions or incompatibilities with ISO/IEC 15408. Any queries are resolved with the applicant. Once this has been done, the status of the entry becomes “registered”, or if an evaluation pass statement or certificate has been confirmed as valid, “evaluated” or “certified” respectively.

If after three months the RA has been unable to resolve all queries and obtain all necessary confirmations, the validation process is abandoned and the entry regraded as “failed validation”.

The normal status of a current register entry is “registered”, “evaluated” or “certified”. If the RA receives valid notification of successful evaluation or certification of a registered PP, the entry status is upgraded to “evaluated” or “certified”. Likewise, if an evaluation pass statement or certificate is withdrawn, the entry is downgraded to “registered”.

Every three years, the sponsor of a registered, evaluated or certified register entry is required to confirm that the entry is still required (and possibly pay an additional fee for continued registration). A check is also made that any evaluation pass statement or certificate is still valid. If the sponsor fails to reply, fails to pay any required fee, or does not wish to continue registration, the status of the entry becomes “obsolescent”.

Obsolescent entries have been withdrawn or abandoned by their sponsors. They remain in the register, but with a warning from their status that they are passing out of valid use. A sponsor can make a registered, evaluated or certified entry obsolescent at any time. If a defect is reported in a complete PP or package, and the sponsor fails to respond to the reported error, the status is also changed to obsolescent as a warning that the entry is no longer being supported by its sponsor.

An entry remains in obsolescent status for 18 months. At the end of this time, it is automatically downgraded to “retired”, indicating that the entry is no longer in active use. Retired entries remain in the register, so that they can be referenced for historical purposes.

© ISO/IEC 2001 – All rights reserved

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

ICS 35.040

Price based on 14 pages

© ISO/IEC 2001 – All rights reserved

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale