
**Information technology — Software asset
management —**

**Part 2:
Software identification tag**

*Technologies de l'information — Gestion de biens de logiciel —
Partie 2: Étiquette d'identification du logiciel*

Withhold

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.

Withdrawn

**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2009

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.org
Web www.iso.org

Published in Switzerland

Table of Contents

Page

Foreword	v
Introduction.....	vi
1 Scope	1
1.1 Purpose	1
1.2 Field of application.....	1
1.3 Limitations	1
2 Conformance	2
2.1 General	2
2.2 Product conformance	2
2.3 Organizational conformance.....	5
2.4 Agreement compliance.....	6
3 Normative references.....	6
4 Terms, definitions and abbreviated terms.....	6
4.1 Terms and definitions	6
4.2 Abbreviated terms	12
5 Alignment and rationalization with prior standards	12
5.1 Statement of alignment for this part of ISO/IEC 19770.....	12
5.2 Alignment with ISO/IEC 19770-1:2006 Information technology — Software asset management — Part 1: Processes	12
5.3 Alignment with ISO/IEC 20000-1:2005 Information technology — Service management — Part 1: Specification	13
5.4 Alignment with ISO/IEC 20000-2:2005 Information technology — Service management — Part 2: Code of practice	14
6 Implementation of software identification tagging processes	14
6.1 General requirements and guidance	14
6.2 Software identification tagging life cycle: operational breakdown.....	22
7 Platform requirements and guidance.....	24
7.1 Types of platforms	24
7.2 Basic platform services	25
7.3 Virtual environments.....	25
7.4 Virtual machines.....	26
7.5 Support for software installed on removable media	26
7.6 Hardware and platform identification.....	26
8 Elements.....	27
8.1 General	27
8.2 Element names	27
8.3 Mandatory elements.....	28
8.4 Optional elements	33
8.5 Extended elements.....	60
8.6 Data type definitions	61
Annex A (informative) Software identification tagging principles.....	67
Annex B (informative) Software provider use cases and guidance	73
Annex C (informative) Tool provider use cases and guidance	78
Annex D (informative) Software consumer use cases and guidance.....	81
Annex E (informative) Software identification tags for items other than software	85
Annex F (informative) Copyright and software identification tags.....	86

Annex G (normative) **XML schema definition (XSD)**.....87
Annex H (informative) **Extended examples**.....95

Figures Page

Figure 1 — Software identification tag lifecycle..... 22
Figure A.1 — Life cycle of a software identification tag..... 67

Tables Page

Table 1 - Examples of regid values15
Table 2 - Examples of tag locations on different platforms16
Table 3 - Microsoft Vista® APIs for software identification tag management.....16

Withold@AMM

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 2.

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 document 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 19770-2 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software and systems engineering*.

ISO/IEC 19770 consists of the following parts, under the general title *Information technology — Software asset management*:

- *Part 1: Processes*
- *Part 2: Software identification tag*
- *Part 3: Software entitlement tag*

Introduction

This part of ISO/IEC 19770 provides an International Standard for software identification tags. The software identification tag is an XML file containing authoritative identification and management information about a software product. The software identification tag is installed and managed on a computing device together with the software product. The tag may be created as part of the installation process, or added later for software already installed without tags. However, it is expected more commonly that the tag will be created when the software product is originally developed, and then be distributed and installed together with the software product. Having the tag available from the beginning allows for the more effective management of distribution and repackaging external to the software consumer, and then of release management within the software consumers organization.

This part of ISO/IEC 19770 supports software asset management processes as defined in ISO/IEC 19770-1. It is also designed to work together with the future ISO/IEC 19770-3 which will provide an International Standard for software entitlement tags.

Software identification tags will benefit all stakeholders involved in the creation, licensing, distribution, releasing, installation, and on-going management of software. Key benefits associated with software identification tags include:

- a) The ability to consistently and authoritatively identify software products that need to be managed for any purpose, such as for licensing, upgrading, packaging or for the specification of dependencies. Software identification tags provide the meta-data necessary to support more accurate identification which differentiates this approach from traditional file-oriented identification techniques.
- b) The ability to identify groups or suites of software products in the same way as for individual software products, enabling entire groups or suites of software products to be managed with the same flexibility as for individual products.
- c) Facilitation of de facto standardization between different software creators, and within software creator organizations, of how different versions of software are identified, allowing for better identification and management by software consumers of those different versions; for example, being able to distinguish between free-standing versions and versions which are components of suites, upgrade paths, etc.
- d) Facilitation of automated approaches to license compliance, using information both from the software identification tag and from the software entitlement tag as will be specified in ISO/IEC 19770-3.
- e) The ability to provide comprehensive information about the structural footprint of packages, i.e. the list of components such as files and system settings associated with that package, in order to link package-level management with file-level management.
- f) The ability to provide information about how to identify if a particular software package is being actively used or not.
- g) The ability to deal with the complexities of software installed on removable or shared storage, or in virtual environments (subject to the evolving ability of platforms and installers to identify devices and environments).
- h) The ability to reflect within the software identification tag the identities and requirements of different entities, including software creators, software licensors, packagers, distributors external to the software consumer, release managers within the software consumer, and those responsible for installing and managing software on an on-going basis.
- i) The ability to allow for the validation of any of this information through the optional use of digital signatures by anyone creating or modifying information in the software identification tag.

- j) The ability for entities besides the software creators (e.g. independent providers, or in-house personnel) to create software identification tags for legacy software, and also for software from software creators who do not provide software identification tags themselves.
- k) The ability of this International Standard to evolve in informal and formal ways, as common approaches become accepted throughout industry for dealing with additional types of information not currently covered by this part of ISO/IEC 19770, such as for product activation.

Withdrawn

Information technology — Software asset management —

Part 2: Software identification tag

1 Scope

1.1 Purpose

This part of ISO/IEC 19770 establishes specifications for tagging software to optimize its identification and management.

1.2 Field of application

This part of ISO/IEC 19770 applies to:

- a) Platform providers: These are the entities which are responsible for the computer or hardware device and/or associated operating system, or virtual environment, on which software may be installed or run. Platform providers which support this part of ISO/IEC 19770 additionally provide tag management capabilities at the level of the platform or operating system.
- b) Software providers: These are the entities that create (“software creators”), package (“software packagers”) or license (“software licensors”) software for distribution or installation. These include software manufacturers, independent software developers, consultants, and repackagers of previously manufactured software. They may also be in-house software developers.
- c) Tag providers: These are the entities that create (“tag creators”) or modify (“tag modifiers”) software identification tags. A tag provider may be part of the software provider organization, or may be a 3rd party organization or the software consumer.
- d) Tag tool providers: These are the entities that may provide any number of tools that create, modify or use software identification tags. These tools include development environments that provide automatically generated software identification tags, installation tools that may create and/or modify tags on behalf of the installation process as well as desktop management tools that may create tags for software that does not have a tag and/or modify tags with release details throughout the software lifecycle. See Annex C for details on how tool providers are likely to use software identification tags.
- e) Software consumers: These are the entities that purchase, install and/or otherwise consume software, and who are intended as one of the major beneficiaries of the improved information provided by the software identification tag as specified in this part of ISO/IEC 19770. See Annex D for details on how software consumers are likely to use software identification tags.

1.3 Limitations

This part of ISO/IEC 19770 does not detail SAM processes required for reconciliation of software entitlements with software identification tags.

This part of ISO/IEC 19770 does not specify product activation or launch controls.

This part of ISO/IEC 19770 is not intended to conflict either with any organization's policies, procedures or standards or with any national laws and regulations. Any such conflict should be resolved before using this part of ISO/IEC 19770.

2 Conformance

2.1 General

Conformance can apply to a product or an organization. For organizational conformance, the scope defined shall cover both the organizational scope as well as the products that are included in the scope.

If a claim of conformance is made for a product or organization, the claim shall specify the scope for which the conformance was tested.

Conformance throughout this clause is most often defined in terms of complying with the requirements of 6.1, 8.3, 8.4, and 8.5. Requirements for platform conformance are also specified in 7.2. There are also normative requirements specified in other subclauses of Clauses 6 and 7, indicated by the use of the word "shall", but these are not included in the coverage of statements of conformance, except to the extent that they are also included in 6.1, 7.2, 8.3, 8.4, or 8.5. Statements including the word 'should' are recommendations but not mandatory.

2.2 Product conformance

2.2.1 Example reasons for product conformance

There are a number of reasons for an organization to seek individual product conformance to this part of ISO/IEC 19770. This may be sought when a specific product is being provided for a market that requires conformance (for example, if government organizations require products to conform to this part of ISO/IEC 19770 in order to be included on a project). It might also be desired by platform providers who want to provide a more secure and auditable tag storage that can be used to identify definitively which end-users installed which software packages.

2.2.2 Product scope

There shall be a clear statement for product scope describing, in unambiguous terms, the software products to which it applies and, where appropriate, clarifying the products to which it does not apply. The product conformance scope may be defined in any way considered appropriate, such as for a specific software product, for all software products, for all software products on specific platforms, for the software products of specified manufacturers and/or for all software products created after a specified date, as long as it is unambiguous. In the case of a product which creates or modifies software identification tags, the scope shall be the product itself and all software produced or modified by the product when tag-conformity functionality is enabled.

2.2.3 Software product conformance

Full conformance for a software product is achieved in one of two ways:

- a) For a product which is installable, full conformance is achieved by demonstrating that all software identification tags installed by it at installation shall comply with all mandatory requirements of this part of ISO/IEC 19770, as specified in 6.1 and 8.3. If optional or extended tag elements are used these shall also comply with requirements as specified in 8.4 and 8.5.

This conformance shall be demonstrated by performing equivalence partitioning with the exit criteria that all tests pass and 100 % equivalence partition coverage of the tag creation/installation is achieved. Equivalence partitions shall be derived from the statement of product scope.

If the software product consists of a package of other software products, then the software product shall retain all component tags and reference all child tag elements, which, under any circumstances, still need to be identified separately (for the purpose of licensing, security or other).

- b) For a product that is distributable but not yet installed, full conformance is achieved by demonstrating that distributable builds are issued with a unique tag that shall comply with all mandatory requirements of this part of ISO/IEC 19770, as specified in 6.1 and 8.3. If optional or extended tag elements are used these shall also comply with requirements as specified in 8.4 and 8.5. The exception to this is that any mandatory elements which are installation-specific are not included.

This conformance shall be demonstrated by performing equivalence partitioning with the exit criteria that all tests pass and 100 % equivalence partition coverage is achieved. Equivalence partitions shall be derived from the statement of product scope.

If the software product consists of a package of other software products, then the software product shall retain all component tags and reference all child tag elements which under any circumstances still need to be identified separately (for the purpose of licensing, security or other).

2.2.4 Third party software identification tag conformance

Third party tag provider organizations may undertake the process of creating software identification tags for any software packages that do not include such tags. This may be done for older software products, shareware/freeware type products, or for companies that decide not to follow this part of ISO/IEC 19770. These tags may be provided to organizations to assist in their software discovery and identification procedures.

Full conformance for third party created software identification tags is achieved by demonstrating that all software identification tags produced by the organization comply with all mandatory requirements of this part of ISO/IEC 19770, as specified in 6.1 and 8.3. If optional or extended tag elements are used these shall also comply with requirements as specified in 8.4 and 8.5. Any new data that is added shall conform to the same standards as those required for installable software conformance.

Conformance for third party created software identification tags requires that the tag providers demonstrate that the software ids they create are unique, and use consistent values for the identification of software providers. The expectation is that the tag providers will maintain a list of unique software providers for all tags created, and that the list includes a consistent software provider regid (that references the provider's domain) and a unique ID (which may be a GUID) for each reference and that these details are used consistently in the created tags.

This conformance shall be demonstrated by performing equivalence partitioning with the exit criteria that all tests pass and 100 % equivalence partition coverage of the tag production is achieved. Equivalence partitions shall be derived both from the range of software that the tag tool shall work on and the corresponding statements of product scope.

2.2.5 Software installer product conformance

Full conformance for a software installer product is achieved by demonstrating that all software identification tags installed by it at installation comply with all mandatory requirements of this part of ISO/IEC 19770, as specified in 6.1 and 8.3. If optional or extended tag elements are used these shall also comply with requirements as specified in 8.4 and 8.5.

This conformance shall be demonstrated by performing equivalence partitioning with the exit criteria that all tests pass and 100 % equivalence partition coverage of the tag creation/installation is achieved. Equivalence partitions shall be derived both from the range of software that is installed and the corresponding statements of product scope.

If the software being installed consists of a package of other software products, then the software product shall retain all component tags and reference all child tag elements which under any circumstances still need to be identified separately (for the purpose of licensing, security or other).

Existing tag values that are provided with distributable software shall not be modified in any way, with some specific exceptions. If a distributed software identification tag is found to be corrupted and that software identification tag does not provide a "validation" routine to fix the tag, a software product may provide options for handling this type of exception that a SAM practitioner can authorize. Based on actions specified by the SAM practitioner, the handling of such exceptions may include actions such as fixing the software identification tag if it is corrupt, deleting the software identification tag if it no longer belongs on the device, or modifying the software identification tag to specify that the software is no longer installed on the device. Should any modifications of the tag be specified by the user, these actions shall be logged and retained by the software product.

It is expected that such products will have the capability to turn this functionality on or off. A statement of product conformance shall apply only to the product with this functionality turned on.

2.2.6 Tag tool conformance

Full conformance for a tag tool is achieved in one of two ways:

- a) Full conformance for a tag tool that installs or modifies installed software identification tags independent of software installation is achieved by demonstrating that all software identification tags installed or modified by the product comply with all mandatory requirements of this part of ISO/IEC 19770, as specified in 6.1 and 8.3. If optional or extended tag elements are used these shall also comply with requirements as specified in 8.4 and 8.5. Any new data that is added shall conform to the same standards as those required for installable software conformance.

This conformance shall be demonstrated by performing equivalence partitioning with the exit criteria that all tests pass and 100 % equivalence partition coverage of the tag production is achieved. Equivalence partitions shall be derived both from the range of software that the tag tool shall work on and the corresponding statements of product scope.

If the software being installed consists of a package of other software products, then the software product shall retain all component tags and reference all child tag elements which under any circumstances still need to be identified separately (for the purpose of licensing, security or other).

Existing tag values that are provided with distributable software shall not be modified in any way, with some specific exceptions. If a distributed software identification tag is found to be corrupted and that software identification tag does not provide a "validation" routine to fix the tag, a software product may provide options for handling this type of exception that a SAM practitioner can authorize. Based on actions specified by the SAM practitioner, the handling of such exceptions may include actions such as fixing the software identification tag if it is corrupt, deleting the software identification tag if it no longer belongs on the device, or modifying the software identification tag to specify that the software is no longer installed on the device. Should any modifications of the tag be specified by the user, these actions shall be logged and retained by the software product.

It is expected that such products will have the capability to turn this functionality on or off. A statement of product conformance shall apply only to the product with this functionality turned on.

- b) For a tag tool that discovers, collects, reports on and uses tags (such as discovery tools, desktop management tools or SAM reconciliation tools), full conformance is achieved by demonstrating the following.
- 1) That all tags available on a computing device are collected. This includes tags that are stored in the common system location as well as tags that are located in the top level directories of software installations.
 - 2) That all tags collected from computing devices and stored in the tool's repository can be shown to include exactly the same information as the contents of the tag located on the computing device from which it was originally collected.
 - 3) If a tag is digitally signed and the corresponding public key is available, that the tool validates the signature and the information that has been signed.

This conformance shall be demonstrated by performing equivalence partitioning with the exit criteria that all tests pass and 100 % equivalence partition coverage of the tag collection/validation is achieved. Equivalence partitions shall be derived both from the range of software that the tool shall analyze and the corresponding statements of product scope.

If the software being installed consists of a package of other software products, then the software product shall retain all component tags and reference all child tag elements which under any circumstances still need to be identified separately (for the purpose of licensing, security or other).

Existing tag values that are provided with distributable software shall not be modified in any way, with some specific exceptions. If a distributed software identification tag is found to be corrupted and that software identification tag does not provide a "validation" routine to fix the tag, a software product may provide options for handling this type of exception that a SAM practitioner can authorize. Based on actions specified by the SAM practitioner, the handling of such exceptions may include actions such as fixing the software identification tag if it is corrupt, deleting the software identification tag if it no longer belongs on the device, or modifying the software identification tag to specify that the software is no longer installed on the device. Should any modifications of the tag be specified by the end-user, these actions shall be logged and retained by the software product.

It is expected that such products will have the capability to turn this functionality on or off. A statement of product conformance shall apply only to the product with this functionality turned on.

2.2.7 Platform conformance

Full conformance for a platform's tag functionality is achieved by demonstrating that it can store software identification tag data centrally and provide the following services with integrity, as specified in 7.2.

- a) Basic functionality: add, modify, read, and delete tag data.
- b) Security: determine which end-user can read, create, delete and modify software identification tags.
- c) Audit functionality: identify which end-user installed, modified or removed a given software configuration item and when the modification occurred.

This conformance shall be demonstrated by performing equivalence partitioning with the exit criteria that all tests pass and 100 % equivalence partition coverage of the tag storage is achieved. Equivalence partitions shall be derived both from the range of software that the platform shall host and the corresponding statements of product scope.

2.3 Organizational conformance

2.3.1 Example reasons for organizational conformance

Organizations could want to conform to this part of ISO/IEC 19770 for a number of reasons. For example, software providers could want to promote their software products as being easier to manage. Also, software consumers could want to show that they are actively managing their software assets and that they can provide accurate information to any reconciliation or audit request.

2.3.2 Organizational scope

There shall be a clear statement for the organizational scope describing, in unambiguous terms, the organizational structure to which it applies and, where appropriate, clarifying the areas to which it does not apply. A statement of organizational scope shall be accompanied by a statement of software product scope.

2.3.3 Software provider conformance

Full conformance for a software provider is achieved by the organization demonstrating that all software within the scope meets the relevant product conformance requirements, as specified in 2.2.3.

2.3.4 Tag tool provider conformance

Full conformance for a tag tool provider is achieved by an organization demonstrating that all software within the scope meets the relevant tool conformance requirements, as specified in 2.2.6.

Furthermore, in order to claim tag tool provider conformance, all tag tools produced by the organization shall be included in the product scope.

2.3.5 Software consumer conformance

Full conformance for an organization that installs software is achieved by demonstrating that there are software identification tags in place for all software in the software consumer organization's product scope and that the software identification tags comply with all mandatory requirements of this part of ISO/IEC 19770, as specified in 6.1 and 8.3. If optional or extended tag elements are used, these shall also comply with requirements in 8.4 and 8.5.

2.4 Agreement compliance

This part of ISO/IEC 19770 may be used to help develop an agreement between a software provider and a software consumer, in which case clauses of this part of ISO/IEC 19770 can be selected for incorporation into the agreement, with or without modification. In such an instance, it is necessary for both parties to comply with their agreement rather than conform to this part of ISO/IEC 19770.

NOTE ISO/IEC's copyright and patent policy extends to all of this part of ISO/IEC 19770 and contents thereof. However, for the specific use of agreement compliance, there is no need to obtain copyright permission.

3 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

[IETF RFC 3986](#), *Uniform Resource Identifier (URI): Generic Syntax*, 2005

[IETF RFC 4646](#), *Tags for Identifying Languages*, 2006

[W3C Recommendation](#), *XML Signature Syntax and Processing (Second Edition)*, 2008

[W3C Recommendation](#), *XML Schema Part 2: Datatypes (Second Edition)*, 2004

[UNSPSC](#), *The United Nations Standard Products and Services Code*