INTERNATIONAL STANDARD

ISO/IEC 19770-2

Second edition
2015-10-01

Corrected version
2017-02

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



Reference number
ISO/IEC 19770-2:2015(E)

© ISO/IEC 2015



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms, definitions, and abbreviated terms **2**
3.1 Terms and definitions 2
3.2 Abbreviated terms 2

4 Conformance **3**
4.1 SWID tag conformance 3
4.2 Application conformance 3
4.3 Platform conformance 3

5 Interoperability guidance **3**
5.1 Overview 3
5.2 SWID tag modification 3
5.3 SWID tag relationships 4
5.3.1 Overview 4
5.3.2 Pre-installation data attribute 4
5.3.3 SWID patch attribute 4
5.3.4 SWID supplemental attribute 5

6 Implementation of software identification tagging processes **6**
6.1 General requirements and guidance 6
6.1.1 XML and XSD 6
6.1.2 SWID tags based on earlier revisions of this part of ISO/IEC 19770 6
6.1.3 SWID tag installation and removal 6
6.1.4 SWID data storage and transmission 6
6.1.5 Unique registration ID (regid) 7
6.1.6 Tag identifier 8
6.1.7 Unique software identification tag file name 8
6.1.8 Software identification tag discovery 8
6.1.9 Languages 8
6.1.10 Authenticity of software identification tags 9
6.1.11 File hash definitions 9
6.1.12 Use of standardized data types in XSD definition 10
6.1.13 Using Evidence or Payload 10
6.1.14 Redistributable software components 10

7 Platform requirements and guidance **10**

8 Elements **11**
8.1 General 11
8.2 Minimum SWID tag data values required 12
8.3 Recommended SWID tag data values 13
8.4 XML element and attribute names 13
8.4.1 Introduction 13
8.4.2 Additional attributes allowed 14
8.5 Data values 14
8.5.1 SoftwareIdentity 14
8.5.2 Entity 18
8.5.3 Evidence 20
8.5.4 Link 20
8.5.5 Meta 25
8.5.6 Payload 26
8.6 Type and attribute definitions 26

© ISO/IEC 2015 – All rights reserved

8.6.1 Directory 26
8.6.2 File 27
8.6.3 FileSystemItem 28
8.6.4 Ownership 30
8.6.5 NMTOKEN and NMTOKENS 30
8.6.6 Process 30
8.6.7 Rel 30
8.6.8 Resource 31
8.6.9 ResourceCollection 31
8.6.10 Role 32
8.6.11 SoftwareMeta 32
8.6.12 Use 34
8.6.13 VersionScheme 35

Annex A (informative) **XSD changes between revisions** **36**

Annex B (normative) **XML schema definition (XSD)** **39**

Annex C (informative) **UML structure of SWID tag schema** **60**

Annex D (informative) **Sample tags** **62**

Bibliography **73**

 © ISO/IEC 2015 – All rights reserved

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 7, *Software and systems engineering*.

This second edition cancels and replaces the first edition (ISO/IEC 19770-2:2009), which has been technically revised.

This corrected version of ISO/IEC 19770-2 incorporates the following corrections plus other minor editorial modifications:

— two subclauses have been added to 8.4; and

— the schema for the BaseElement type has been replaced in Annex B.

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

— *Part 1: Processes and tiered assessment of conformance*

— *Part 2: Software identification tag*

— *Part 5: Overview and vocabulary*

The following parts are under preparation:

— *Part 3: Software entitlement schema*

— *Part 4: Resource Utilization Measurement (RUM)*

— *Part 7: Tag management*

The following part is planned:

— *Part 22: Guidance for the use of* ISO/IEC 19770-2 *Software Identification Tag information in Cyber Security*

© ISO/IEC 2015 – All rights reserved

Introduction

Overview

International Standards in the ISO/IEC 19770 family of standards for Information Technology (IT) asset management (ITAM) address both the processes and technology for managing software, hardware, and related IT assets. Because IT is an essential enabler for almost all activity in today's world, these standards must integrate tightly into all of IT. For example, software identification (SWID) tags have the capacity to assist in other management functions outside the scope of financial-focused or compliance-focused ITAM processes. From a technology perspective, ITAM standards for information structures provide not only the data interoperability of software management data, but also provide the basis for many related benefits such as more effective security in the management of software. ITAM standards for information structures also facilitate significant automation of IT functionality, such as improved authentication of software and automated linking to identify vulnerability information for more automated exposure identification and mitigation.

Purpose of this part of ISO/IEC 19770

This part of ISO/IEC 19770 provides an International Standard for software identification tags. The software identification tag is a standardized data structure containing software identification information about a software product that supports new and automated management functions. Product information provided in the software identification tag structure will often be provided in an XML data file, but the same SWID tag product information may be accessible through other means depending on the computing device being managed.

SWID tags are created by a SWID tag producer, for example a software creator who develops and distributes software or a tool and/or service provider. SWID tag data is utilized by SWID tag consumers, for example a discovery tool or service that collects information from a computing device for a variety of purposes such as license compliance, software security, or logistics operations. Providing authoritative and detailed software identification information makes the management of software less expensive and provides support for significantly more automation for IT processes in the security, compliance, and logistics areas.

This part of ISO/IEC 19770 has been developed to facilitate automation of IT processes through the use of software identification tags and for applications which use those tags, for the purposes of security, compliance, and logistics automation. This part of ISO/IEC 19770 includes information which facilitates human intelligibility (such as edition and colloquial version name), but it is unrealistic to expect to create, manage, and use software identification tags without the use of automated capabilities built into specialist or generalist tools. The extent to which such capabilities are provided by specialist commercial products, open-source-type products, or platforms themselves, will depend on market developments over time.

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

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 the following.

a) The ability to consistently and authoritatively identify software products that need to be managed for any purpose, such as for licensing, security, logistics, or for the specification of dependencies. Software identification tags provide the meta-data necessary to support more accurate identification than other software identification techniques.

b) The ability to identify groups or suites of software products in the same way as individual software products, enabling entire groups or suites of software products to be managed with the same flexibility as individual products.

 © ISO/IEC 2015 – All rights reserved

c) The ability to automatically relate installed software with other information such as patch installations, configuration issues, or other vulnerabilities.

d) Facilitate interoperability of software information between different software creators, different software platforms, different IT management tools, and within software creator organizations, as well as between SWID tag producers and SWID tag consumers.

e) Facilitate automated approaches to license compliance, using information both from the software identification tag and from the software entitlement schema as specified in ISO/IEC 19770-3.

f) Provide a comprehensive information structure of the structural footprint of products, for example the list of software components of files and system settings associated with a product to identify if files have been modified.

g) Provide a comprehensive information structure that identifies different entities, including software creators, software licensors, packagers, distributors external to the software consumer, as well as various entities within the software consumer, associated with the installation and management of the product on an on-going basis.

h) Through the optional use of digital signatures by organizations creating software identification tags, the ability to validate that information is authoritative and has not been maliciously tampered with.

i) The opportunity for entities other than original software creators (e.g. independent providers or in-house personnel) to create software identification tags for legacy software, and for software from software creators who do not provide software identification tags themselves.

This part of ISO/IEC 19770 is divided into the following clauses and annexes:

— Clause 1 defines the scope;

— Clause 2 describes the normative references;

— Clause 3 describes the terms, definitions, and abbreviated terms used in this part of ISO/IEC 19770;

— Clause 4 defines conformance;

— Clause 5 provides interoperability guidance;

— Clause 6 describes the implementation of software identification tagging processes;

— Clause 7 contains platform implementation requirements and guidance;

— Clause 8 describes the elements of the tag;

— Annex A contains information on why the changes to the SWID tag schema are necessary;

— Annex B contains the XML schema document for the tag;

— Annex C provides a UML diagram of the SWID tag schema;

— Annex D provides sample tags.

© ISO/IEC 2015 – All rights reserved

Information technology — Software asset management —

Part 2: Software identification tag

1 Scope

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

This part of ISO/IEC 19770 applies to the following.

a) Tag producers: these organizations and/or tools create software identification (SWID) tags for use by others in the market. A tag producer may be part of the software creator organization, the software licensor organization, or be a third-party organization. These organizations and/or tools can broadly be broken down into the following categories.

   1) Platform providers: entities responsible for the computer or hardware device and/or associated operating system, virtual environment, or application platform, on which software may be installed or run. Platform providers which support this part of ISO/IEC 19770 may additionally provide tag management capabilities at the level of the platform or operating system.

   2) Software providers: entities that create, license, or distribute software. For example, software creators, independent software developers, consultants, and repackagers of previously manufactured software. Software creators may also be in-house software developers.

   3) Tag tool providers: entities that provide tools to create software identification tags. For example, tools within development environments that generate software identification tags, or installation tools that may create tags on behalf of the installation process, and/or desktop management tools that may create tags for installed software that did not originally have a software identification tag.

b) Tag consumers: these tools and/or organizations utilize information from SWID tags and are typically broken down into the following two major categories:

   1) software consumers: entities that purchase, install, and/or otherwise consume software;

   2) IT discovery and processing tool providers: entities that provide tools to collect, store, and process software identification tags. These tools may be targeted at a variety of different market segments, including software security, compliance, and logistics.

This part of ISO/IEC 19770 does not prescribe Information Technology Asset Management (ITAM) or other IT-related processes required for reconciliation of software entitlements with software identification tags or other IT requirements.

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 or international laws and regulations.

2 Normative references

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

© ISO/IEC 2015 – All rights reserved

ISO/IEC 19770–5, *Information technology — Software asset management — Part 5: Overview and vocabulary*

IEEE 1003.1:2013, *Standard for Information Technology — Portable Operating System Interface (POSIX(R))*

W3C Recommendation, *XML Schema Part 2: Datatypes (Second Edition)*

IETF RFC 3986, *Uniform Resource Identifier (URI): Generic Syntax*

3 Terms, definitions, and abbreviated terms

3.1 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19770-5 and the following apply.

3.1.1
patch
software component that, when installed, directly modifies files or device settings related to a different software component without changing the version number or release details for the related software component

3.1.2
platform provider
organization responsible for the platform

Note 1 to entry: The platform provider is typically the vendor of the relevant operating system, virtual environment, or application platform.

3.1.3
tagId
globally unique value that shall be globally unique for every SWID tag created

Note 1 to entry: Globally unique values may use a 16 byte GUID, or other globally unique value as defined by the tag creator.

3.2 Abbreviated terms

API application programming interface

GUID globally unique identifier

IETF Internet Engineering Task Force

MD5 message digest 5

regid registration identifier

RPC remote procedure call

SAM software asset management

SHA secure hash algorithm

SWID software identification, or software identification tag

URI uniform resource identifier

URL uniform resource locator

© ISO/IEC 2015 – All rights reserved