INTERNATIONAL STANDARD

ISO/IEC 17960

First edition
2015-09-01

Information technology — Programming languages, their environments and system software interfaces — Code signing for source code

Technologies de l'information — Langages de programmation, leur environnement et interfaces des logiciels de systèmes — Signature numérique pour le code source

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 17960:2015
https://standards.iteh.ai/catalog/standards/sist/b0c5c051-46b6-45b4-8721-3149a991453a/iso-iec-17960-2015

Reference number
ISO/IEC 17960:2015(E)

© ISO/IEC 2015

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 17960:2015
https://standards.iteh.ai/catalog/standards/sist/b0c5c051-46b6-45b4-8721-3149a991453a/iso-iec-17960-2015

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 17960:2015
https://standards.iteh.ai/catalog/standards/sist/b0c5c051-46b6-45b4-8721-3149a991453a/iso-iec-17960-2015

© ISO/IEC 2015 – All rights reserved

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

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 ISO documents 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 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

ISO/IEC 17960, was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 22, *Programming languages, their environments and system software interfaces*.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 17960:2015
https://standards.iteh.ai/catalog/standards/sist/b0c5c051-46b6-45b4-8721-3149a991453a/iso-iec-17960-2015

© ISO/IEC 2015 – All rights reserved

Introduction

Source code is written and is used in many critical applications. Knowing that the source code being relied upon is the same as that which was used in testing is vital to ensuring the safety and security of a particular application. Given the ease with which source code can be modified, some method of protecting the integrity and authenticity of the source code is necessary. Sequestration of the source code throughout the supply chain is one possible method, but ensuring protection in that way is impractical and unreliable. Virtual protection through the use of a digital signature offers a practical solution and provides integrity and authentication even though the source code may traverse an insecure supply chain.

Source code may be modified for legitimate reasons as it moves through the supply chain or over time. Modifications to source code may be made to correct the software or to adapt it for other purposes. Modifications may only involve changes to a few lines of code and in most cases is not made by the original author or team of authors. Revision control software facilitates tracking of the software changes, but such tracking can easily be spoofed. The use of a digital signature provides a means to restrict the ability to spoof. Digital code signing assigns a responsible party to each revision of the source code and thus can demonstrate the authenticity of the responsible party, the source code and the software changes that have been made between revisions. By doing this, an electronic pedigree for the source code can be established.

This standard specifies the process for signing source code in order to ensure the integrity and authenticity of the source code and a means for rolling back the source code to signed previous versions. Clause 5 provides an overview of the concepts of code signing. Conformance requirements for this standard are specified in Clause 6. Annex A is informative and provides a step by step description of a typical application for the standard specified in Clause 6 to assist in understanding code signing. The bibliography lists documents that were referenced during preparation of this standard.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 17960:2015
https://standards.iteh.ai/catalog/standards/sist/b0c5c051-46b6-45b4-8721-3149a991453a/iso-iec-17960-2015

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO/IEC 17960:2015
https://standards.iteh.ai/catalog/standards/sist/b0c5c051-46b6-45b4-8721-3149a991453a/iso-iec-17960-2015

INTERNATIONAL STANDARD **ISO/IEC 17960:2015(E)**

Information technology — Programming languages, their environments and system software interfaces — Code signing for source code

1 Scope

This International Standard specifies a language-neutral and environment-neutral description to define the methodology needed to support the signing of software source code, to enable it to be uniquely identified, and to enable roll-back to signed previous versions. It is intended to be used by originators of software source code and the recipients of their signed source code. This International Standard is designed for transfers of source code among disparate entities.

The following areas are outside the scope of this International Standard:

- Determination of the trust level of a certification authority;
- Format used to track revisions of source code files;
- Digital signing of object or binary code;
- System configuration and resource availability;
- Metadata
  - This is partially addressed by ISO/IEC 19770-2;
- Transmission and representation issues
  - Though this could be an issue in implementation, there are techniques such as Portable Document Format (PDF)[1] that can be used to mitigate these issues. This applies in particular to the transmission of digital signatures.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 17960:2015
https://standards.iteh.ai/catalog/standards/sist/b0c5c051-46b6-45b4-8721-3149a991453a/iso-iec-17960-2015

2 Conformance

An implementation of code signing conforms to this International Standard if it meets the requirements specified in Clause 6.

3 Normative references

The following documents, in whole or in part, are normatively referenced in this standard 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 9594-8:2014, *Information technology — Open Systems Interconnection — The Directory — Part 8: Public-key and attribute certificate frameworks*[2]

ISO/IEC 10118-3:2004, *Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash functions*

[1] ISO 32000-1:2008 Document management — Portable document format — Part 1: PDF 1 specifies a digital form for representing electronic documents to enable users to exchange and view electronic documents independent of the environment in which they were created or the environment in which they are viewed or printed.

[2] This is equivalent to ITU-T Recommendation X.509: 2005, "*Information Technology —Open Systems Interconnection — The Directory: Public-Key and attribute certificate frameworks*"

ISO/IEC 13888-1:2009, *Information technology — Security techniques — Non-repudiation — Part 1: General*

4 Terms and definitions

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

4.1
certificate
entity's data rendered unforgeable with the private or secret key of a certification authority

[SOURCE: ISO/IEC 13888-1:2009]

4.2
certification authority
authority trusted by one or more users to create and assign certificates

[SOURCE: ISO/IEC 13888-1:2009]

4.3
changeset
set of all changes that are applied to a configuration to derive a new configuration

4.4
digital signature
data appended to, or a cryptographic transformation of, a data unit that allows the recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 17960:2015
https://standards.iteh.ai/catalog/standards/sist/b0c5c051-46b6-45b4-8721-3149a991453a/iso-iec-17960-2015

[SOURCE: ISO/IEC 13888-1:2009]

4.5
hash code
string of bits that is the output of a hash-function

[SOURCE: ISO/IEC 13888-1:2009]

4.6
hash-function
function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: 1) it is computationally infeasible to find for a given output an input which maps to this output; 2) it is computationally infeasible to find for a given input a second input which maps to the same output

[SOURCE: ISO/IEC 13888-1:2009]

4.7
originator
entity that sends a message to the recipient or makes available a message for which non-repudiation services are to be provided

[SOURCE: ISO/IEC 13888-1:2009]

4.8
private key
key of an entity's asymmetric key pair which should only be used by that entity

[SOURCE: ISO/IEC 13888-1:2009]

© ISO/IEC 2015 – All rights reserved

4.9
public key
key of an entity's asymmetric key pair which can be made public

[SOURCE: ISO/IEC 13888-1:2009]

4.10
public key certificate
public key information of an entity signed by the certification authority and thereby rendered unforgeable

[SOURCE: ISO/IEC 13888-1:2009]

4.11
recipient
entity that gets (receives or fetches) a message for which non-repudiation services are to be provided

[SOURCE: ISO/IEC 13888-1:2009]

4.12
snapshot
complete copy of a configuration

5 Concepts

This clause provides an overview of the concepts of code signing.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Code signing is a technique for providing a digital signature for source code to support a verification of the originator and a verification that the code has not been altered since it was signed.

Code signing can provide several valuable functions such as:

ISO/IEC 17960:2015
https://standards.iteh.ai/catalog/standards/sist/b0c5c051-46b6-45b4-8721-3149a991453a/iso-iec-17960-2015

- knowledge of the history of the source code
- confidence that the source code has not been accidentally or maliciously altered
- verification of the identity of the responsible party for the source code
- accountability for the source code
- non-repudiation of the originator of the source code

Code signing identifies to customers the responsible party for the source code and confirms that it has not been modified since the signature was applied. Verification of the originator of the source code of the software is extremely important since the security and integrity of the receiving systems can be compromised by faulty or malicious code. In addition to protecting the security and integrity of the software, code signing provides authentication of the author, originator or distributor of the source code, and protects the brand and the intellectual property of the developer of the software by making applications uniquely identifiable and more difficult to falsify or alter maliciously.

When source code is associated with an originator's unique signature, distributing source code on the Internet is no longer an anonymous activity. Digital signatures ensure accountability, just as a manufacturer's brand name ensures accountability with packaged software. Distributions on the Internet lack this accountability and code signing provides a means to offer the needed accountability. Accountability can be a strong deterrent to the distribution of harmful code. Even though software may be acquired or distributed from an untrusted site or a site that is unfamiliar, the fact that it is signed by a known and trusted entity allows the software to be used with confidence that it has not been changed as compared to the most recently signed version.