

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*

---

---

Reference number  
ISO/IEC 17960:2015(E)





**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

This is a preview of "ISO/IEC 17960:2015". Click here to purchase the full version from the ANSI store.

## Contents

	Page
<b>Foreword</b> .....	<b>iv</b>
<b>Introduction</b> .....	<b>v</b>
<b>1 Scope</b> .....	<b>1</b>
<b>2 Conformance</b> .....	<b>1</b>
<b>3 Normative references</b> .....	<b>1</b>
<b>4 Terms and definitions</b> .....	<b>2</b>
<b>5 Concepts</b> .....	<b>3</b>
<b>6 Requirements</b> .....	<b>4</b>
6.1 General .....	4
6.2 Certificates .....	4
6.3 Hash code .....	5
6.4 Initial code signing .....	5
6.5 Modifying signed previous versions .....	5
6.6 Revision format .....	5
<b>Annex A (informative) Notional code signing process</b> .....	<b>6</b>
<b>Bibliography</b> .....	<b>7</b>

## 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](http://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](http://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*.

This is a preview of "ISO/IEC 17960:2015". [Click here to purchase the full version from the ANSI store.](#)

## 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.