TECHNICAL REPORT

ISO/IEC TR 24485

First edition
2022-10

Information security, cybersecurity and privacy protection — Security techniques — Security properties and best practices for test and evaluation of white box cryptography

Sécurité de l'information, cybersécurité et protection de la vie privée — Techniques de sécurité — Propriétés de sécurité et bonnes pratiques pour les essais et l'évaluation de la cryptographie en boîte blanche

Reference number
ISO/IEC TR 24485:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

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.

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 or www.iec.ch/members_experts/refdocs).

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) or the IEC list of patent declarations received (see https://patents.iec.ch).

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

The white box cryptography (WBC) is a specific implementation method for cryptographic algorithms where the secret key and the algorithm are entangled, so that the user can freely stimulate the latter. However, the secret key is deeply engraved in the implementation, such that it is hard to extract and is unambiguous. Furthermore, it is also difficult to update the WBC implementation in order to change the key.

WBC is typically used for implementation when secure cryptographic module functionality (such as a tamper-resistance device or a physically unclonable function) is unavailable for the protection of secrets.

Business cases include DRM (digital right management) and HCE (host card emulation), in the contexts of media protection and payment applications. WBC implementations are widely deployed on mobile devices, where the cryptographic implementation is provided over the top.

The purpose of this document is to provide best practices on security assurance and to facilitate users to assess the security level of several WBC implementations. It is important to share common information and best practices about test and evaluation of WBC security.

Information security, cybersecurity and privacy protection — Security techniques — Security properties and best practices for test and evaluation of white box cryptography

1 Scope

This document introduces security properties and provides best practices on the test and evaluation of white box cryptography (WBC). WBC is a cryptographic algorithm specialized for a key or secret, but where the said key cannot be extracted.

The WBC implementation can consist of plain source code for the cryptographic algorithm and/or of a device implementing the algorithm. In both cases, security functions are implemented to deter an attacker from uncovering the key or secret.

Security properties consist in the secrecy of security parameters concealed within the implementation of the white box cryptography. Best practices for the test and evaluation includes mathematical and practical analyses, static and dynamic analyses, non-invasive and invasive analyses.

This document is related to ISO/IEC 19790 which specifies security requirements for cryptographic modules. In those modules, critical security parameters (CSPs) and public security parameters (PSPs) are the assets to protect. WBC is one solution to conceal CSPs inside of the implementation.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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.

ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*