TECHNICAL SPECIFICATION

ISO/IEC TS 19608

First edition
2018-10

Guidance for developing security and privacy functional requirements based on ISO/IEC 15408

Lignes directrices pour l'élaboration des exigences fonctionnelles de sécurité et de confidentialité fondées sur l'ISO/IEC 15408

Reference number
ISO/IEC TS 19608:2018(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
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. 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 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.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

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.

Introduction

ISO/IEC 29100 defines a framework of privacy principles that should be considered when developing systems or applications that deal with personally identifiable information (PII). This document analyses those principles and maps them, where possible, to the security functional requirements defined in ISO/IEC 15408-2. Where such a mapping is not possible, this document derives new security functional requirements collected in one new class that contains several families of privacy related security functional components following the guidance for developing new classes, families and components provided in ISO/IEC 15408-1 and ISO/IEC 15408-2.

This document can also be used as guidance for developing further privacy functional requirements using the framework of ISO/IEC 15408. The class, families, and components defined in this document can be extended for cases where the components defined here are not sufficient to express specific privacy functional requirements.

Guidance for developing security and privacy functional requirements based on ISO/IEC 15408

1 Scope

This document provides guidance for:

— selecting and specifying security functional requirements (SFRs) from ISO/IEC 15408-2 to protect Personally Identifiable Information (PII);

— the procedure to define both privacy and security functional requirements in a coordinated manner; and

— developing privacy functional requirements as extended components based on the privacy principles defined in ISO/IEC 29100 through the paradigm described in ISO/IEC 15408-2.

The intended audience for this document are:

— developers who implement products or systems that deal with PII and want to undergo a security evaluation of those products using ISO/IEC 15408. They will get guidance how to select security functional requirements for the Security Target of their product or system that map to the privacy principles defined in ISO/IEC 29100;

— authors of Protection Profiles that address the protection of PII; and

— evaluators that use ISO/IEC 15408 and ISO/IEC 18045 for a security evaluation.

This document is intended to be fully consistent with ISO/IEC 15408; however, in the event of any inconsistency between this document and ISO/IEC 15408, the latter, as a normative standard, takes precedence.

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 15408-1, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 18045, *Information technology — Security techniques — Methodology for IT security evaluation*

ISO/IEC 29100, *Information technology — Security techniques — Privacy framework*