INTERNATIONAL STANDARD

ISO/IEC 27034-5

First edition
2017-10

Information technology — Security techniques — Application security —

Part 5: Protocols and application security controls data structure

Technologies de l'information — Techniques de securite — Securite des applications —

Partie 5: Protocoles et structure de données de contrôles de sécurité d'application

Reference number
ISO/IEC 27034-5:2017(E)

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

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 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 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 the following URL: 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*.

A list of all parts in the ISO/IEC 27034 series can be found on the ISO website.

Introduction

General

There is an increasing need for organizations to focus on protecting their information at the application level. A systematic approach towards increasing the level of application security provides an organization with evidence that information being used or stored by its applications is being adequately protected.

ISO/IEC 27034 (all parts) provides concepts, principles, frameworks, components and processes to assist organizations in integrating security seamlessly throughout the life cycle of their applications.

The Application Security Control (ASC) is one of the key components of this document.

To facilitate the implementation of ISO/IEC 27034 (all parts) application security framework and the communication and exchange of ASCs, a minimal set of essential attributes should be documented and explained for realizing ASCs and certain other components of the framework.

This document explains the minimal set of essential attributes of ASCs and further details the Application Security Life Cycle Reference Model (ASLCRM).

Purpose

The purpose of this document is to document and explain the essential information and data structure requirements for ASCs. The advantages of a standardized set of essential information attributes and data structure of ASCs include the following:

a) normalized ASC creation, communication, protection and verification in compliance with the requirements of this document; and

b) minimized cost of security in application projects by facilitating the reuse of approved controls and acquisition of ASCs from different sources."

In addition, this document defines and details the processes, activities and roles involved in the Application Security Life Cycle Reference Model.

Targeted audiences

General

The following audiences will find values and benefits when carrying their designated organizational roles:

a) managers;

b) ONF committee;

c) domain experts;

d) suppliers; and

e) acquirers.

Managers

Managers should read this document because they are responsible for:

a) ensuring the ASCs are reusable within the organization, and

b) ensuring the ASCs are available, communicated and used in application projects with proper tools and procedures all across the organization.

Organization Normative Framework (ONF) Committee

The ONF Committee is responsible for managing the implementation and maintenance of the application-security-related components and processes in the Organization Normative Framework. The ONF Committee:

a) implements the ASC Library,

b) approves ASCs that correctly mitigate application security risks, and

c) manages the cost of implementing and maintaining the ASCs.

Domain experts

Domain experts contribute knowledge in application provisioning, operating or auditing, who:

a) participate in ASC development, validation and verification,

b) participate in ASC implementation and maintenance, by proposing strategies, components and implementation processes for adapting ASCs to the organization's context, and

c) validate that ASCs are useable and useful in application projects.

Security tools and ASC supplier

Suppliers contribute to develop, maintain and distribute tools and/or ASCs. They

a) create, validate, enforce integrity (through a recognized method, such as signing), distribute and apply ASCs, and

b) align with a common and standardized exchange protocol (structure and format) for ASCs.

Security tools and ASC acquirer

Acquires are individuals or organizations who want to acquire ASCs. They

a) integrate ASCs into their organization and ensure the interoperability of any internal and third-party ASCs,

b) adapt ASCs and enforce their integrity, and

c) ensure that the activities and tasks of acquired ASCs can be mapped to the organization’s application lifecycle.