TECHNICAL SPECIFICATION

# ISO/IEC TS 27034-5-1

First edition
2018-04

# Information technology — Application security —

## Part 5-1: Protocols and application security controls data structure, XML schemas

*Technologies de l'information — Sécurité des applications —*

*Partie 5-1: Protocoles et structure de données de contrôles de sécurité d'application, schémas XML*



Reference number
ISO/IEC TS 27034-5-1:2018(E)

© ISO/IEC 2018



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
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** ... **iv**
**Introduction** ... **v**
**1 Scope** ... **1**
**2 Normative references** ... **1**
**3 Terms and definitions** ... **1**
**4 Abbreviated terms** ... **1**
**5 XML Schema for ASCs** ... **2**
5.1 General ... 2
5.2 Global design decisions ... 2
5.3 General XML Information ... 2
5.4 ASC Data Model Definition ... 3
5.4.1 General ... 3
5.4.2 ASC Package ... 3
5.4.3 ASC Element ... 8
5.4.4 ASC Identification ... 12
5.4.5 ASC Objective ... 16
5.4.6 ASC Security activity and Verification measurement ... 21
5.4.7 Complex type `asc:activity` ... 21
5.4.8 Complex type `asc:actor` ... 37
5.4.9 Complex type `asc:information` ... 40
5.4.10 Complex type `asc:ASLCRM_activity-name` ... 42
5.4.11 Enumeration types ... 55

© ISO/IEC 2018 – All rights reserved

# 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 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 Joint 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.


© ISO/IEC 2018 – All rights reserved

# Introduction

## 0.1 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 ISO/IEC 27034 (all parts). To facilitate the implementation of the ISO/IEC 27034 (all parts) application security framework and the communication and exchange of ASCs, a formally defined exchange format is required.

This documents is a Technical Specification document and defines XML Schemas of essential attributes of ASCs and further details the Application Security Life Cycle Reference Model.

## 0.2 Purpose

The purpose of this document is to define XML schemas that implement the essential information and data structure requirements for ASCs as well as the Application Security Lifecycle Reference Model (ASLCRM). The advantages of a standardized set of essential information attributes and data structure of ASCs include the following:

a) facilitate the exchange of application security controls (ASCs);

b) provide a formally defined reference model for tool vendors, ASC suppliers and acquirers.

## 0.3 Targeted audiences

### 0.3.1 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;

e) acquirers.

### 0.3.2 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.

### 0.3.3 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 needs to:

a) implement the ASC Library;

© ISO/IEC 2018 – All rights reserved

b) approve ASCs that correctly mitigate application security risks; and

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

### 0.3.4 Domain experts

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

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.

### 0.3.5 ASC suppliers

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

a) create, validate, sign, distribute and apply ASCs; and

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

### 0.3.6 ASC acquirers

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

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

b) adapt and sign ASCs to enforce their integrity; and

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

 © ISO/IEC 2018 – All rights reserved

# Information technology — Application security —

# Part 5-1: Protocols and application security controls data structure, XML schemas

## 1 Scope

This document defines XML Schemas that implement the minimal set of information requirements and essential attributes of ASCs and the activities and roles of the Application Security Life Cycle Reference Model (ASLCRM) from ISO/IEC 27034-5.

## 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 27034-1, *Information technology — Security techniques — Application security — Part 1: Overview and concepts*

ISO/IEC 27034-5, *Information technology — Security techniques — Application security — Part 5: Protocols and application security control data structure*

## 3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 27034-1 and the following apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

**3.1**
**activity**
set of actions or tasks carried out by an actor during the application's lifecycle

## 4 Abbreviated terms

| | |
|---|---|
| ASC | Application Security Control |
| ASLC | Application Security Life Cycle |
| ASLCRM | Application Security Life Cycle Reference Model |
| ICT | Information and Communication Technology |
| ONF | Organization Normative Framework |

© ISO/IEC 2018 – All rights reserved