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 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 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.

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;

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.

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

5 XML Schema for ASCs

5.1 General

The purpose of Clause 5 is to define an XML implementation of the information requirements and essential attributes for ASC identified in ISO 27045-5. The schema source file can be downloaded from ISO.

5.2 Global design decisions

In line with the objectives and requirements defined in ISO/IEC 27034-5, the following high-level design decisions for this implementation of the ASC data model were taken:

a) **XML and XML schema:** ASCs are defined in the platform-independent extensible markup language (XML). Consequently, the data model for ASCs is defined in the form of an XML schema;

b) **ASC package:** The data model provides a mechanism for grouping and bundling one or many related ASCs in form of an *ASC package*. This allows for the convenient exchange of related ASCs;

c) **Level of Trust inclusion:** Each ASC should refer to one or more levels of trust. In order to keep the ASC self-contained the data model is designed to also include the actual definition of the levels of trust.

5.3 General XML Information

All XML elements defined by the XML Schema for the ASC data model are part of "asc" namespace and shall be qualified by asc. The namespace URI for this specification should be "http://standards.iso.org/iso-iec/ts/27034/5-1/ed-1/en". Applications that process ASCs should use the namespace URI to decide whether or not they can process a given document. The XML schema implementation defined in this subclause should be the authoritative XML binding definition for ASCs.

Table 1 — ASC Data Model — Namespace and Schema Import Definition

```
<?xml version="1.81" encoding="UTF-8"?>
<!-- edited for ISO/IEC 27034 by Luc Poulin and Daniel Sinnig -->
<xs:schema
   xmlns:asc="http://iso.org/ISO27034/ASC-structure"
   xmlns:xs="http://www.w3.org/2001/XMLSchema"
   xmlns:aslcrm="http://iso.org/ISO27034ASLCRM"
   targetNamespace="http://iso.org/ISO27034/ASC-structure"
   elementFormDefault="qualified"
   attributeFormDefault="qualified"
   version="1.0RC">
   ...
</xs:schema>
```

NOTE 1 ASC developers align their vocabulary with ISO/IEC 19770 (all parts) when they need to describe assets.

NOTE 2 Explicit indication of an inheritance hierarchy is not implemented in the ASC structure, but can be implemented in future versions.

5.4 ASC Data Model Definition

5.4.1 General

The purpose of 5.4 is to present an overview of all structural elements defined by the XML schema for the ASC structure. The elements are presented in a top-down manner where high-level elements are successively refined into lower-level elements. All XML elements defined in this XML Schema are part of the “asc” namespace and shall be qualified by `asc`:

5.4.2 ASC Package

5.4.2.1 General

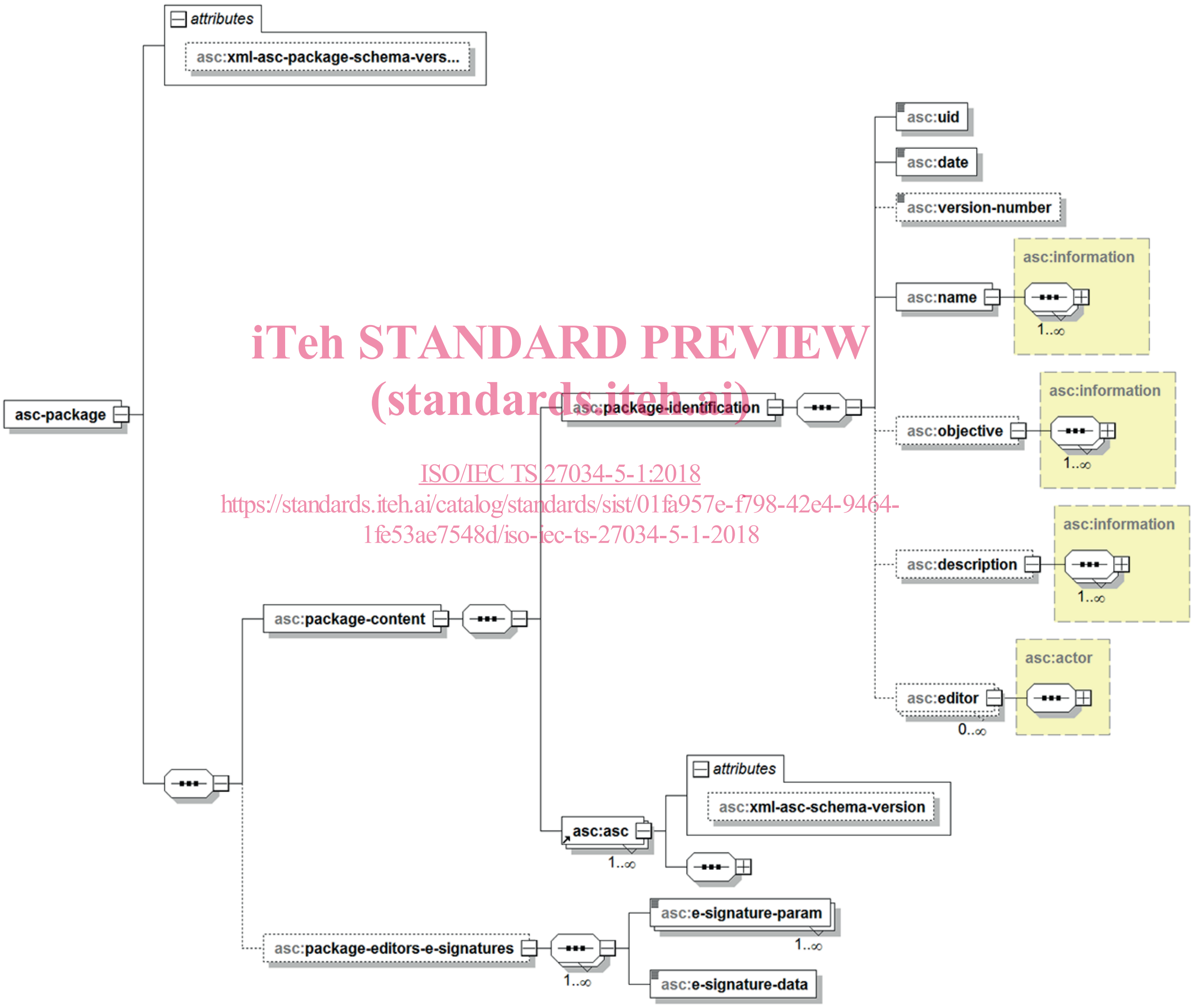

Figure 1 — ASC Package

The top-level element `<asc:asc-package>` mechanism for grouping and bundling one or many related ASCs in form of an ASC package (Figure 1). This allows for the convenient exchange of related ASCs. It consists of the following sub-elements:

a) `<asc:package-content>` is actual payload of the package. It consists of package meta-data <asc:package-content> and one or more ASCs <asc:package-content>;

b) `<asc:package-editors-e-signatures>` optionally contains digital signatures to validate the source and integrity of the entire package.

NOTE The ASC package object and the ASC object both have a schema version number value defined in the XML-Schema used to identify their data structure. It consists of the following attributes:

a) `<asc:xml-asc-package-schema-version>`; and

b) `<asc:xml-asc-schema-version>`.

Table 2 shows the implementation of the element `<asc:asc-package>` in the XML Schema.

Table 2 — `<asc:asc-package>` element

```
<xs:element name="asc-package">
   <xs:complexType>
      <xs:sequence>
         <xs:element name="package-content">
            <xs:complexType>
               <xs:sequence>
                  <xs:element name="package-identification">
                     <xs:complexType>
                        <xs:sequence>
                           <xs:element name="uid" type="xs:string">
                           </xs:element>
                           <xs:element name="date" type="xs:date">
                           </xs:element>
                           <xs:element name="version-number"
                                       type="xs:string" minOccurs="0">
                           </xs:element>
                           <xs:element name="name" type="asc:information">
                           </xs:element>
                           <xs:element name="objective"
                                       type="asc:information" minOccurs="0">
                           </xs:element>
                           <xs:element name="description"
                                       type="asc:information" minOccurs="0">
                           </xs:element>
                           <xs:element name="editor" type="asc:actor"
                                       minOccurs="0" maxOccurs="unbounded">
```

Table 2 *(continued)*

```
                           </xs:element>
                        </xs:sequence>
                     </xs:complexType>
                  </xs:element>
                  <xs:element ref="asc:asc" maxOccurs="unbounded">
                  </xs:element>
               </xs:sequence>
            </xs:complexType>
         </xs:element>
         <xs:element name="package-editors-e-signatures" minOccurs="0">
            <xs:complexType>
               <xs:sequence maxOccurs="unbounded">
                  <xs:element name="e-signature-param" type="xs:string"
                              maxOccurs="unbounded">
                  </xs:element>
                  <xs:element name="e-signature-data" type="xs:string">
                  </xs:element>
               </xs:sequence>
            </xs:complexType>
         </xs:element>
      </xs:sequence>
      <xs:attribute name="xml-asc-package-schema-version" type="xs:string"
                    default="1.0.0.0">
      </xs:attribute>
   </xs:complexType>
</xs:element>
```

5.4.2.2 ASC Package Content

The `<asc:package-content>` elements consists of meta-data information about its contents and one more more ASCs. It consists of the following sub-elements.

a) `<asc:package-identification>` defines meta-date information about the package contents such uid, date, version, name, objective, description and editor;

b) `<asc:asc>` defines a particular ASC. Each ASC package is required to have one or more `<asc:asc>` elements.

Table 3 shows the implementation of the element `<asc:package-content>` in the XML Schema.

Table 3 — `<asc:package-content>` element

```
<xs:element name="package-content">
   <xs:complexType>
      <xs:sequence>
         <xs:element name="package-identification">
            <xs:complexType>
               <xs:sequence>
                  <xs:element name="uid" type="xs:string">
                  </xs:element>
                  <xs:element name="date" type="xs:date">
                  </xs:element>
                  <xs:element name="version-number" type="xs:string"
                              minOccurs="0">
                  </xs:element>
                  <xs:element name="name" type="asc:information">
                  </xs:element>
                  <xs:element name="objective" type="asc:information"
                              minOccurs="0">
                  </xs:element>
                  <xs:element name="description" type="asc:information"
                              minOccurs="0">
                  </xs:element>
                  <xs:element name="editor" type="asc:actor" minOccurs="0"
                              maxOccurs="unbounded">
                  </xs:element>
               </xs:sequence>
            </xs:complexType>
         </xs:element>
         <xs:element ref="asc:asc" maxOccurs="unbounded">
         </xs:element>
      </xs:sequence>
   </xs:complexType>
</xs:element>
```

5.4.2.3 ASC Package identification

The element `<asc:package-identification>` contains meta-data information about the ASC package. It consists of the following elements:

a) `<asc:uid>` is a unique identifier of the ASC package;

b) `<asc:date>` is the date the package was created (combined date and time in UTC following ISO 8601);

c) `<asc:version-number>` optionally denotes the version of the package;

d) <asc:name> is the name of the package. This element has the custom type asc:information (defined in 5.4.9) used to specify the localization (i.e. language, area, organization) of the information contained by this <asc:name> element;

e) <asc:objective> optionally describes the objective or theme of the package;

f) <asc:description> optionally provides an informal (localized) description of the package;

g) <asc:editor> optionally defines the editor of the package. This element has the custom type asc:actor (defined in 5.4.8) used to specify the name and coordinates of the author.

Table 3 shows the implementation of the element <asc:package-identification> in the XML Schema.

5.4.2.4 ASC Package e-signature

The element <asc:package-editors-e-signatures> contains digital signatures of the <asc:package-content> element. Each digital signature consists of one or more e-signature parameters and the actual e-signature.

a) <asc:e-signature-param> defines relevant parameters about the e-signature such as signature algorithm, key size, hashing algorithm and the public key used to validate the signature; and

b) <asc:e-signature-date> contains the actual digital signature of the asc-package.

Table 4 shows the implementation of the element <asc:package-editors-e-signatures> in the XML Schema.

Table 4 — <asc:package-editors-e-signatures> element

```
<xs:element name="package-editors-e-signatures" minOccurs="0">
   <xs:complexType>
      <xs:sequence maxOccurs="unbounded">
         <xs:element name="e-signature-param" type="xs:string"
                     maxOccurs="unbounded">
         </xs:element>
         <xs:element name="e-signature-data" type="xs:string">
         </xs:element>
      </xs:sequence>
   </xs:complexType>
</xs:element>
```

5.4.3 ASC Element

5.4.3.1 General

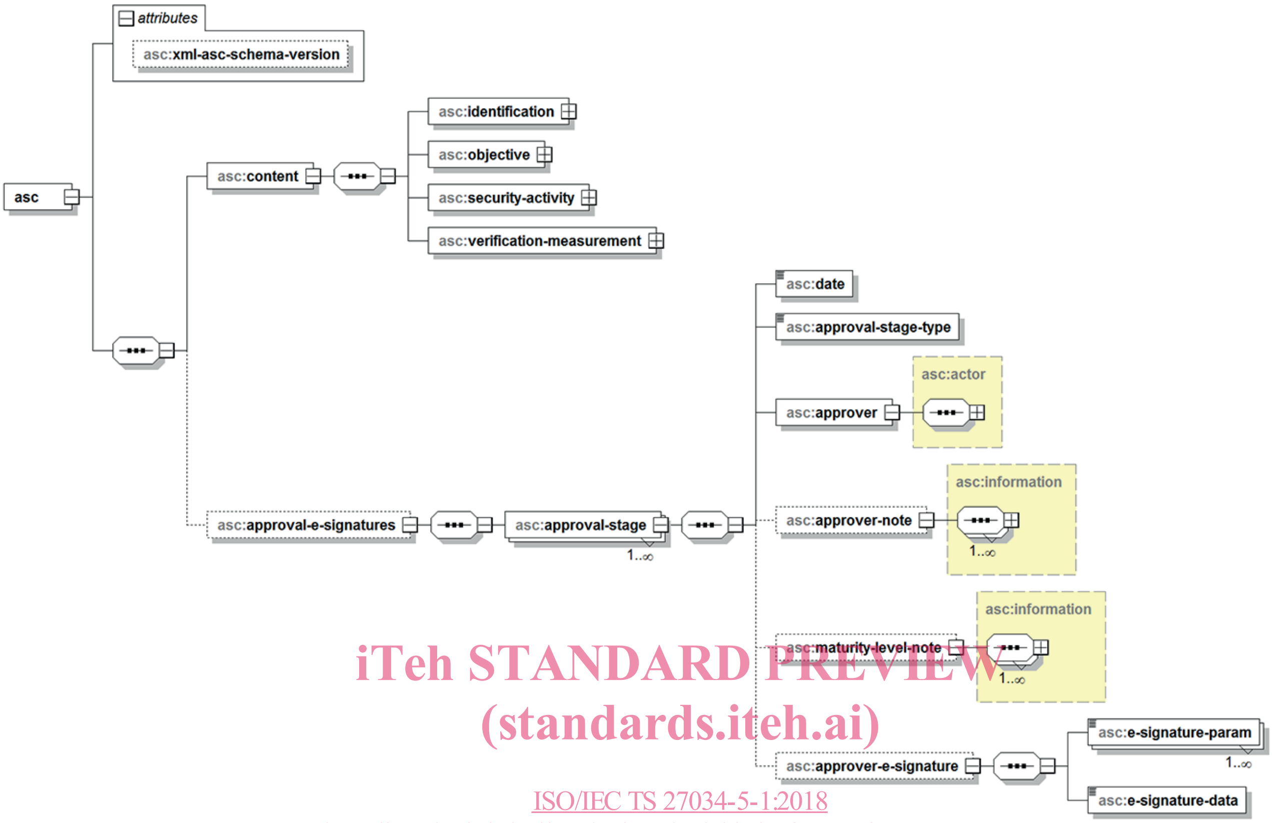

Figure 2 — ASC Top Level Structure

The <asc:asc> element holds all information pertinent to one application security control (ASC). The <asc:asc> element contains the attribute xml-asc-schema-version. It identifies the version of the XML schema the (instance) XML document is compatible with. It also contains the following two sub-elements:

a) <asc:content> contains the actual ASC information contents;

b) <asc:approval-e-signature> optionally contains the actual digital signature and related information to clarify and to protect the ASC contents.

5.4.3.2 ASC Content

The element <asc:content> defines the actual ASC (see Figure 2). It consists of the following elements:

a) <asc:identification> defines information related to the identity of the ASC such as uid, name, version, date, author and owner (defined in 5.4.4);

b) <asc:objective> defines key attributes including description, addressed security requirements, assigned levels of trust, relationships to other ASCs, etc (defined in 5.4.5);

c) <asc:security-activity> defines the activity that needs to be carried out to address the security requirements associated with the ASC. High-level ASCs may not explicitly define a security activity. In such a case the definition of the activity is deferred to a lower-level ASC. The <asc:security-activity> element is assigned the complex type asc:activity (defined in 5.4.7);

d) `<asc:verification-measurement>` defines the activity that needs to be carried out to verify the security activity. High-level ASCs may not explicitly define a verification measurement. In such a case the definition of the activity is deferred to a lower-level ASC. The `<asc:verification-measurement>` is assigned the complex type `asc:activity` (defined in 5.4.7).

Table 5 shows the implementation of the element `<asc:content>` in the XML Schema.

Table 5 — `<asc:content>` element

```
<xs:element name="content">
   <xs:complexType>
      <xs:sequence>
         <xs:element name="identification">
            ...
         </xs:element>
         <xs:element name="objective">
            ...
         </xs:element>
         <xs:element name="security-activity" type="asc:activity">
            ...
         </xs:element>
         <xs:element name="verification-measurement" type="asc:activity">
            ...
         </xs:element>
      </xs:sequence>
   </xs:complexType>
</xs:element>
```

5.4.3.3 ASC approval-e-signatures

The element `<asc:asc-approval-e-signature>` contains the digital signature of the `<asc:package-content>` which can be signed at different ASC life-cycle stages (e.g., design, development, verification, final approval, etc). For each signed stage, a separate signature is provided (see Figure 2). Therefore the element consists of one ore more `<asc:approval-stage>` elements — each contains the signature for one particular ASC lifecycle stage and consists of the following elements:

a) `<asc:date>` denotes the date when the ASC was signed;

b) `<asc:approval-stage-type>` denotes the lifecycle stage of the ASC for which the signature was generated. It is assigned the custom enumeration type `asc:life-cycle-stage` (defined in 5.4.11);

c) `<asc:approver>` contains information about the actor that has approved and signed the ASC. This element has the custom type `asc:actor` (defined in 5.4.8) used to specify the name and coordinates of the author;

d) `<asc:approver-note>` optionally contains optional additional information provided by the approver of the ASC;