

10 Evidence Elements

10.1 Evidence Elements Class Diagram

This sub clause defines the key concepts of the SACM Evidence Metamodel. The elements in this sub clause are defined as abstract classes and subsequent sub clauses elaborate the detail, while this sub clause provides a convenient outline of the entire vocabulary focusing at the key noun concepts.

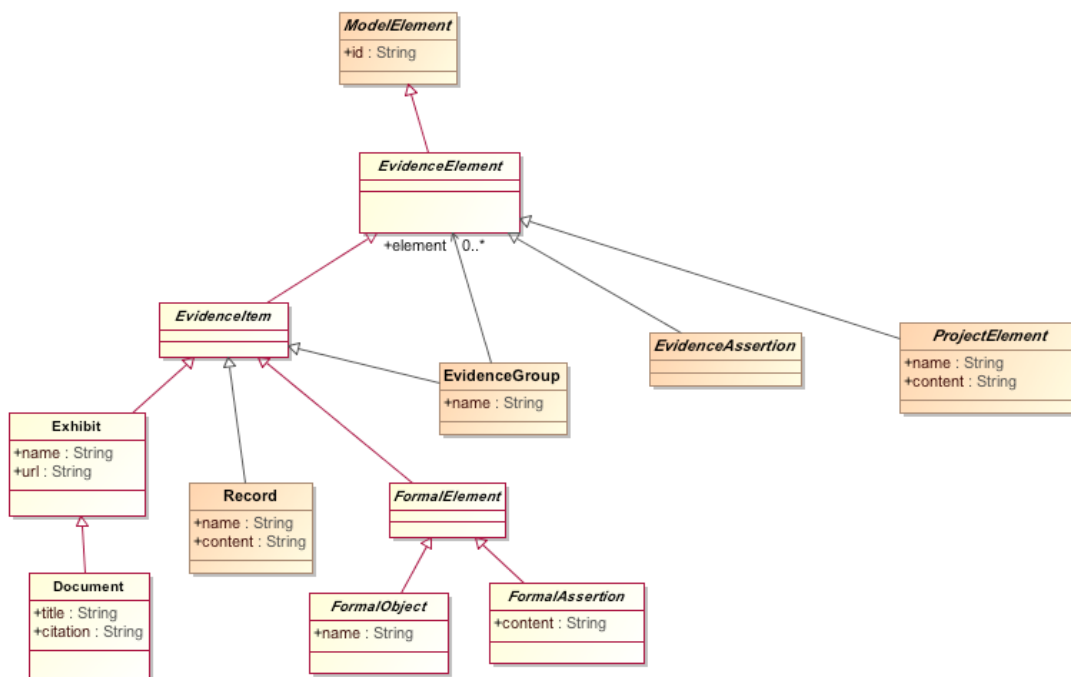


Figure 10.1 - EvidenceElements class diagram

10.1.1 EvidenceElement (abstract)

EvidenceElement class is the root element of the SACM Evidence Metamodel. All other classes in the SACM Evidence Metamodel extend EvidenceElement. The main subclass of the EvidenceElement is EvidenceItem, which defines the primary elements of the Evidence Metamodel. Other elements represent various secondary elements and dependent parts of other evidence elements. The following elements are direct subclasses of EvidenceElement: EvidenceItem, EvidenceAssertion, and ProjectElement.

(statements about things and other statements)

Superclass

(things)

ModelElement

Associations

- provenance:Provenance[0..*]

Provenance properties of the EvidenceElement

statements where the subject is the current EvidenceElement

may be used as a subject of various statements identifying its characteristics, provenance, custody, and other properties. These statements are represented by owned EvidenceProperty elements (see sections 11 and 13 for more detail).

- timing:TimingProperty[0..*] statements where the subject is the current EvidenceElement
Timing properties of the EvidenceElement
- custody:CustodyProperty[0..*] statements where the subject is the current EvidenceElement
Custody properties of the EvidenceElement
- event:EvidenceEvent[0..*] statements sub clauses
Event properties describing a set of events with timing clauses determined by the lifecycle of the EvidenceElement.

Note: This is the complete list of associations for EvidenceElement as they are introduced by several other diagrams of the Evidence Metamodel.

Semantics

EvidenceElement class is an abstract class that represents any element of the SACM Evidence Metamodel. Every class of the SACM Evidence Metamodel extends EvidenceElement directly or indirectly (through other classes).

EvidenceElement may own certain EvidenceProperties. When an EvidenceElement owns an EvidenceProperty, the property represents a relationship between the current EvidenceElement object and some other object referenced by the corresponding EvidenceProperty. Similarly, EvidenceElement may own certain EvidenceAttribute. When an EvidenceElement owns an EvidenceAttribute, the attribute represents a relationship between the current EvidenceElement object and some other object that is referenced by the corresponding EvidenceAttribute.

10.1.2 EvidenceItem (abstract)

EvidenceItem is an abstract class that represents objects that are collected as evidence or are somehow involved with evidence being collected. These objects are either physical documents, records, formal objects (representing concrete objects or concepts), or formal assertions (see below). EvidenceItem owns a set of events that represent the lifecycle and the chain of custody of the item.

The very nature of evidence is that some physical objects called “exhibits” are produced to provide justification to the claims made in an argument. This form of justification conferred by a physical object to a claim is called evidentiary support. So, the main evidence item is an Exhibit - a physical object produced believed to be conferring evidentiary support to some claims in the argument.

The most common form of an exhibit is a Document. Document is a special object, because it is a direct expression of some meaning in certain media. In Software Assurance, most documents are electronic, however some documents may exist on paper or any other media. In comparison any other physical object may represent a meaning only in a very indirect way. Physical objects other than documents require non-trivial (and highly contestable) interpretation, as to what meaning they may represent. Classes Exhibit and Document are described below. Statements related to their properties, are represented by the subclasses of the abstract class ExhibitProperties and DocumentProperties are described in Clause 11 “Exhibit Properties.”

Superclass

EvidenceElement

Semantics

EvidenceItem represents objects that are collected as evidence. The subclasses of EvidenceItem are Exhibit, representing physical objects presented as evidence, Record, EvidenceGroup and FormalElement, which represents associated elements of meaning, such as concepts and propositions/claims.

is associated with a set of statements, which assert some additional facts about that element, including

things

objects

thing

is believed

Instances of concrete subclasses of EvidenceItem are owned by EvidenceContainer (see section 15 Administration).

statements involving this element can be constructed, for example statements that assert fundamental characteristics of this element or its

10.1.3 Exhibit

Exhibit element represents a physical **object** presented as evidence because it is believed to confer evidential support to some claims. Exhibit element in the Evidence Metamodel is a representative of this physical **object** within the Evidence Model, so that **additional properties can be attached to it, and so that it can participate in** various relationships with other elements of the Evidence Model. The nature of Exhibit as something that is presented as evidence and subsequently stored in an appropriate evidence repository, provides the scope of what can be presented as evidence. For example, a “knife” can be presented as evidence, but a person cannot be. A person can have viewed as a witness or an expert, and his opinion recorded as a document, which then can be presented as evidence. The SACM Evidence Metamodel emphasizes computer-based evidence repositories, which can only store electronic representations of physical **objects**. So the “electronic source” of a “knife” **object** will likely be a photograph of the knife.

A most common kind of an exhibit is a Document. Document is a special **object**, because it is a direct expression of some meaning in certain media. Document involves the use of a language to express its meaning. In comparison any other physical **object** may represent a meaning only in a very indirect way. Physical **objects** require non-trivial (and highly contestable) interpretation, as to what meaning they may represent. The importance of documents as elements of evidence cannot be underestimated, since evidentiary support is a form of establishing defensible relation between some physical **objects** and claims, which are elements of meaning. This transition from physical **objects** to meanings needs to be performed as early as possible in the process of building an assurance case. The Evidence Metamodel provides the means to document this transition and confine it to the scope of the evidence package, so that the rest of an assurance case can operate only with claims as elements of meaning, rather than with any physical **objects**, including documents.

The Evidence Metamodel defines some common properties of exhibits including the name (short title) of the exhibit, electronic source of the exhibit, the media (the material of the **object**).

Superclass

EvidenceItem

Attributes

- name:String
The short title of the exhibit.
- url:String
The URL to the original exhibit, if it is a web resource.

Associations

- property:ExhibitProperty[0..*]
The set of essential properties of the exhibit.

Semantics

Exhibit element represents a physical **object** that is presented as evidence in support of some claims. **Properties of an Exhibit are defined as attributes of the Exhibit class itself, as well as the owned elements of the ExhibitProperty class. Each subclass of the ExhibitProperty class owned by an Exhibit object defines a characteristic of the exhibit, represented by the Exhibit object.**

10.1.4 Document

Document element represents a “document” that is defined as follows:

1. an original or official paper relied on as the basis, proof, or support of something;
2. something (as a photograph or a recording) that serves as evidence or proof;
3. a) a writing conveying information; b) a material substance (as a coin or stone) having on it a representation of thoughts by means of some conventional mark or symbol [Merriam-Webster Dictionary].

thing

Document element is the main subclass of Exhibit. Document is a special **object**, because it is a direct expression of some meaning in certain media. In Software Assurance, most documents are electronic, however some documents may exist on paper or any other media. Document involves the use of a language to express its meaning. In comparison any other physical **object** may represent a meaning only in a very indirect way. Physical **objects** require non-trivial (and highly contestable) interpretation, as to what meaning they may represent. FormalAssertion and FormalObject on the other hand are representations of some meaning rather than of an expression of a meaning (direct or indirect). FormalObject may refer to some physical **objects** as its extent but it may not correspond to any physical object whatsoever. From this perspective, a Document is a vital kind of a physical object, which is related directly to some meaning, and requires only a limited interpretation. The importance of documents as elements of evidence cannot be underestimated, since evidentiary support is a form of establishing defensible relation between some physical **objects** and claims, which are elements of meaning. This transition from physical **objects** to meanings needs to be performed as early as possible in the process of building an assurance case. The Evidence Metamodel provides the means to document this transition and confine it to the scope of the evidence package, so that the rest of an assurance case can operate only with claims.

The SACM Evidence Metamodel defines some common properties of documents, such as Title, version, language, etc. Several properties are defined as attributes of the class Document, others are defined as owned properties through named association classes, which are concrete subclasses of DocumentProperty. In addition, the Evidence Metamodel allows several attributes of a Document that characterize its quality as evidence.

Superclass

Exhibit

Attributes

- title:String
The full title of the document
- citation:String
The full citation of the document (bibliographical reference)

Additional facts related to the Document are asserted as DocumentProperty statements in which the current Document is the subject. These statements are represented as owned DocumentProperty elements.

Semantics

thing

Document element represents a physical **object** that directly expresses a certain meaning. The meaning is the content of the document. Because of the ambiguity of natural languages, some documents may express more than one meaning. Formal documents usually have a single meaning. Properties of a Document defines attributes of the Document class itself, as well as the owned elements of the DocumentProperty class. Each subclass of the DocumentProperty class owned by a Document object defines a characteristic of the document, represented by the Document object.

10.1.5 Record

Record element represents Exhibits that are explicit records of compliance, for example log entries. Record is different from a Document, since a Document element represents some physical **object** that exists elsewhere in the physical world (even if it is an electronic document), while a Record element exists only in the EvidenceContainer.

thing

Superclass

EvidenceElement

Attributes

- name:String
the name of the record
- content:String
the content of the record

Semantics

Record is defined as “a thing constituting a piece of evidence about the past, esp. an account of an act or occurrence kept in writing or some other permanent form.” In the Evidence Metamodel Record element is such a thing. In contrast to a Document element, a Record is not a representative of some other physical **object**, but the **object** itself. A Record is therefore similar to an Object; however, it is considered a structured element with an informal content rather than a formal element.

thing

10.1.6 FormalElement (abstract)

FormalElement is an abstract class that represents any elements of meaning that are associated with **objects** presented as evidence or otherwise involved in the evidence collection.

things

Superclass

EvidenceItem

Semantics

FormalElement is an element of meaning that represents a certain individual concept, a noun concept, verb phrases, and propositions. Two subclasses of FormalElement are FormalObject, representing noun concepts, and FormalAssertion, representing verb concepts and propositions.

things

10.1.7 FormalObject (abstract)

FormalObject is an abstract class that represents any elements of meaning that are noun concepts associated with the **objects** that are collected as evidence or are otherwise involved in the evidence collection. FormalObject may represent a concept corresponding to an individual concrete physical thing, such as “an axe with stains of blood on it,” or a collection of things, referred to as a whole, or a concept, such as a “murder weapon.” Physical things need to be represented as the exhibits. On the other hand, concepts are usually not collected as evidence, rather they are used as the elements of meaning in order to build assertions, as well as other relations describing the items of evidence. For example, in order to describe the above mentioned “axe” as a “murder weapon,” the instance of a FormalObject with the name “murder weapon” is used. This object represents a concept that is involved in making a claim that also involves a concrete physical **object**. FormalObjects represent concepts in the subject area for which the argument is being developed. Many elements of the Evidence Metamodel are concepts related to evidence. In particular, Exhibit and Document are two key concepts related to evidence.

thing

Superclass

FormalElement

Attributes

- name:String
Name of the domain concept

Further details are provided in section 12
Formal Statements.

Semantics

FormalObject is an element of meaning that represents a certain individual concept (other than a document) or a noun concept.

10.1.8 FormalAssertion (abstract)

FormalAssertion is an abstract class that represents propositions that are involved in evidence collection. In particular, FormalAssertion involves FormalObject that represents individual concepts corresponding to concrete physical things, collection of things, referred to as a whole, or concepts. FormalAssertions represent propositions about the subject area for which an assurance case is being developed. In contrast, many elements of the Evidence Metamodel are assertions about evidence. In particular, EvidenceEvaluation is one of the key assertions related to evidence.

Superclass

FormalElement

Attributes

- content:String
The statement that in a selected language that is the expression of the formal assertion (verbalization of the assertion in a natural language).

Further details are provided in section 12
Formal Statements.

Semantics

FormalAssertion is an element of meaning that represents a certain proposition. The Assertion subclass, introduced in Clause 12 “Formal Statements” uses elements of formal statements and a formal reference to an SBVR vocabulary to represent precise meaning of the assertion. ReferencedClaim element represents an informal assertion/claim.

10.1.9 EvidenceGroup

EvidenceGroup asserts a state of affairs that several evidence elements are grouped together and can be referred to collectively.

Superclass

EvidenceItem

Attributes

- name:String
Name of the evidence group.

Associations

- element:EvidenceElement [0..*]
Elements of the Evidence Group

- Attributes of the evidentiary support, such as Direct or indirect support, Relevance, Confidence, Strength, Significance.
- Interpretation of Evidence: what an evidence item “Is,” what it “means.”
- Nature of the evidentiary support: Supports, Challenges.
- Observations and Resolutions.
- Standard of Proof to which the evidence is evaluated.

The EvidenceProperty statement is formed by combining the owning EvidenceElement with the objects into the sentential form determined by the concrete subclass of the EvidenceProperty element. See section 13 Evidence Properties for detail.

Superclass

EvidenceElement

Semantics

EvidenceAssertion is an abstract class that represents various **assertions-related to** evidence elements defined in the Evidence Metamodel. More detailed semantics is provided by the concrete subclasses of EvidenceAssertions.

statements about the

10.2.2 EvidenceProperty (abstract)

EvidenceProperty represents various statements related to the fundamental properties of evidence elements.

Superclass

EvidenceAssertion

Semantics

EvidenceProperty is owned by the subject EvidenceElement. EvidenceProperty is a statement that represents fundamental properties of the EvidenceElement. Such properties are independent of the particular assurance case, for example, the media of a document, the current custodian of the document, or the author of a statement. EvidenceProperty involves one or more objects, specified either as attributes or the associations of the EvidenceProperty element. **Each EvidenceProperty represents a relationship between the subject Element that owns it and the corresponding objects.**

In contrast, EvidenceEvaluation elements represent various statements related to the nature of evidentiary support

10.2.3 EvidenceEvaluation (abstract)

allows constructing statements asserting relationships between

Establishing evidentiary support that a set of documents provides to the given claim requires evaluation of the documents and its relations to the claims, including the detection of challenges to the claim, conflicts, and contradictions. Satisfying a certain standard of proof requires analysis of all available evidence items and resolving/explaining conflicts, so that at the end all evidence points in a single direction. Often this requires formulation of a multitude of intermediate claims that are clearly supported by available evidence items and establishing further relations to the target claim.

EvidenceEvaluation is an abstract element that **represents relationships between** evidence items and assertions, observations regarding conflicts, and resolutions of the conflicts. Navigation through the EvidenceEvaluation elements for the given domain claim allow understanding the exact nature and strength of the evidentiary support provided by the evidence items to the claim. **EvidenceEvaluation elements are subjects for additional EvidenceProperty clauses.**

Superclass

EvidenceAssertion

Additional EvidenceProperty and EvidenceAttribute clauses can be added to EvidenceEvaluation statements to provide further detail related to strength, confidence, provenance, timing, etc.

Instances of concrete subclasses of EvidenceEvaluation are owned directly by EvidenceContainer (see section 15 Administration)

Associations

- attribute:EvidenceAttribute[0..*]
Set of quality attributes of this EvidenceEvaluation element.

Semantics

~~EvidenceEvaluation establishes relationship between endpoints, such as between EvidenceItems, as well as between EvidenceEvaluation elements themselves. EvidenceAttribute elements owned by the EvidenceEvaluation determine the properties of the relation between the endpoints of the EvidenceEvaluation.~~



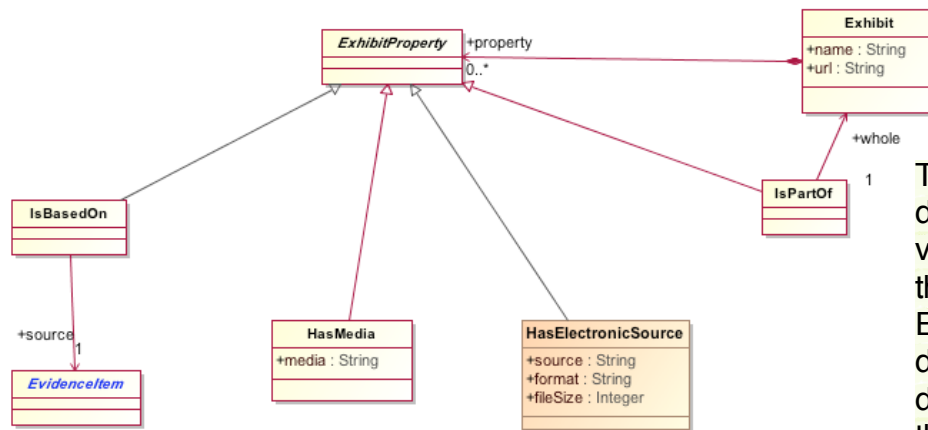
EvidenceEvaluation element represents a statement that asserts a certain relationship between two EvidenceItems, or between an EvidenceItem and an EvidenceEvaluation, or between two EvidenceEvaluations elements. The EvidenceEvaluation statement can include additional EvidenceAttribute clauses, that provide further detail related to confidence, strength of support, etc. Since EvidenceEvaluation element is a subclass of EvidenceElement, the primary statement can also include additional EvidenceProperty clauses that provide further detail related to provenance, timing, etc.

EvidenceAttribute class is further described in section 14.3. Detailed semantics is provided for individual subclasses of EvidenceEvaluation (see section 14 EvidenceEvaluation).

11 Exhibit Properties

This sub clause of the Evidence Metamodel specification defines elements that allow constructing statements about the fundamental properties of Exhibits and Documents.

11.1 ExhibitProperties Class Diagram



The ExhibitProperties class diagram defines several very generic statements about the properties of Exhibit. Subsequent class diagram DocumentProperties defines statements about the properties of Document (a special subclass of Exhibit).

Figure 11.1 - ExhibitProperties class diagram

11.1.1 Exhibit Property (abstract)

This class defines common physical characteristics of exhibits, including documents.

Superclass

EvidenceProperty

Semantics

Each concrete subclass of ExhibitProperty defines a certain statement that identifies a characteristic of exhibit. The subject of the statement is the instance of Exhibit that owns the ExhibitProperty element. The ExhibitProperty statement is formed by combining the owning Exhibit with the corresponding objects into the sentential form determined by the concrete subclass of the ExhibitProperty element. See subsequent sections for detail.

Each concrete subclass of ExhibitProperty defines a single characteristic of the exhibit. An instance of a concrete subclass of the ExhibitProperty class that is owned by some Exhibit object defines a characteristic of the exhibit represented by the Exhibit object.

11.1.2 HasElectronicSource

statement expresses the

HasElectronicSource represents the expression of an Exhibit in electronic form. Electronic Source is the only way a document may be stored in a computer based Evidence Repository. For example, Electronic Source can be a photograph of an object, a scanned image of a document, a Word document, an XMI representation of a model. In a general case of a non-document exhibit, the electronic source is likely to be some image of the original object. If the physical object existed in electronic form (as specified by the Media property), then the Electronic Source can be considered the “original” representation of the Exhibit. This is often the case with documents. In the case of documents as exhibits, the concern is to capture the expression of the meaning represented by the document. If the physical document existed in electronic form as some kind of text (as specified by the Media property), then the Electronic Source can be considered the “original” expression of the Exhibit. In other cases, the Electronic Source is a “derived” expression, which can be a source of errors leading to incorrect interpretation of the meaning of the document. Some arguments involve physical evidence where the transformation between a physical object and its electronic form may be contested, especially if the electronic form is used to interpret the meaning of the document. For example, if the original document is a handwritten note on a napkin,

the original electronic source may be a photographic image of the note. However before the meaning of the note can be analyzed, the text version of the note has to be presented. This may involve some degree of interpretation (was this letter “g” or letter “q”?). In this case the text version of the note is a different electronic source. In most cases related to Software Assurance, electronic source in the form of text is either the original media, or the transformation is reliable.

Superclass

ExhibitProperty

Attributes

- source:String
The bytestream representing the owner exhibit in electronic form.
- format:String
The format used by the source.
- fileSize:Integer
The size of the bytestream (in bytes).

identifies the bytestream that is interpreted as the electronic form of the Exhibit

Constraints

- Exhibit shall not have more than one HasElectronicSource property.

Semantics

statement involves three related properties

element that provide the detail of

HasElectronicSource element represents three related properties of the owner Exhibit object, corresponding to the electronic representation of the exhibit. The source property establishes a relationship between the owner Exhibit object and bytestream, which is interpreted as the electronic form of the Exhibit. The source uses the format, and the source has size. We do not make a distinction between single byte character and multi-byte character representations in case of text-based documents. These distinctions shall be made by the format property. The source within the HasElectronicSource property shall represent the entire exhibit, therefore it is not allowed for the exhibit to have more than one electronic source. If an argument requires reference to alternative electronic sources, for example, images at different resolution, the evidence model needs to be more explicit, and include the original exhibit and two derived documents, describing the process of derivation. This allows clear representation of detailed interpretation of each document, unambiguous representation of claims supported by both documents, and evaluation of their contribution to the main claim.

The main characteristic is expressed by a sentential form “Exhibit has electronic source.”

11.1.3 IsPartOf

The statement

Exhibit is provided in format as source

Some exhibits may have complex structure in which different parts render evidentiary support to different claims, and/or have different properties. The SACM Evidence Metamodel allow representing each part of the complex exhibit as a separate Exhibit element, to represent the aggregated whole by another Exhibit element and to represent “part-whole” associations using the “IsPartOf” property.

Superclass

statement

ExhibitProperty

Associations

- whole:Exhibit[1]
The Exhibit object that represents the “aggregated whole” to which the current Exhibit object is a part of.

Semantics

The statement

IsPartOf is a characteristic of Exhibit-1 (instance of a Exhibit class, referred to as the owner of the characteristic), which is defined as a state of affairs that the Exhibit-1 is part from another Exhibit-2.

This characteristic is expressed by a sentential form “Exhibit-1 is part of Exhibit-2.” Exhibit-1 may be part of multiple other exhibits, besides Exhibit-2, and Exhibit-2 may have other exhibits as its parts.

11.1.4 HasMedia

It is often important to identify a particular media of the document or the material of the exhibit. ExhibitProperty HasMedia shall be used for this purpose.

Superclass

statement shall

ExhibitProperty

Attributes

- media:String
Designator of the media of the original Exhibit.

Semantics

statement

HasMedia element represents a characteristic of the owner Document object that identifies the media of the original exhibit. The version property establishes a relationship between the owner Document object and the designation of the media of the original exhibit.

The main characteristic is expressed by a sentential form “Exhibit is made of media” or “Document is expressed on media.”

statement

11.1.5 IsBasedOn

statement describes the sources of the subeject Exhibit

In Software Assurance documents are often generated by automated process from some sources. For example, the probabilities of Faults are generated from a Fault Tree model through the process of Fault Tree analysis. IsBasedOn element allows to represent the relationship between the owner document and its sources. From the evidentiary quality perspective the fact that the owner document was generated from other documents by means of some automated process does not necessarily make it a “secondary” source, as the transformation usually adds value and generates some primary information, not available in the sources (at least not explicitly). However, this usually makes the document “derived,” rather than “original,” since the transformation is a potential source of errors. A document may be based on multiple sources, each of which shall be represented as a separate IsBasedOn property of the owned document.

Superclass

ExhibitProperty

Associations

- source:EvidenceItem[1]
The source document that contributes to the content of the owner document.

Semantics

IsBasedOn is a characteristic of Document-1 (instance of a Document class, referred to as the owner of the characteristic), which is defined as a state of affairs that the content of the Document-1 is derived from another Document-2.

This statement is expressed by

Exhibit

This characteristic is expressed by a sentential form “Document-1 is based on Document-2.” Document-1 may be based on multiple other documents, besides Document-2.

Derivation of one Document from another can have various meanings including, but not limited to the following:

- Version derives from prior version
- Version derives from these versions of items
- Copy
- Uses information from
- Conclusion based on
- Change together or should change if other changes
- Uses
- Subsumes
- Compiled from or otherwise results from tool processing of
- Analysis result regarding
- Obtains resources from
- Share contents

This list is by no means exhaustive and not all may apply to a set of exhibits of interest. Apparently, as natures of dependencies could vary multiple relations related to a single dependent element are possible. The SACM Evidence Metamodel does not provide a normative enumeration of the nature of dependency. However, should an author of a SACM document desire so, a TaggedValue mechanism shall be used for this purpose with a tag ‘natureofdependency.’

The DocumentProperties class diagram defines statements about properties of Documents (a special subclass of Exhibit). DocumentProperty is defined as a subclass of a more generic ExhibitProperty class (see previous section).

11.2 DocumentProperties Class Diagram

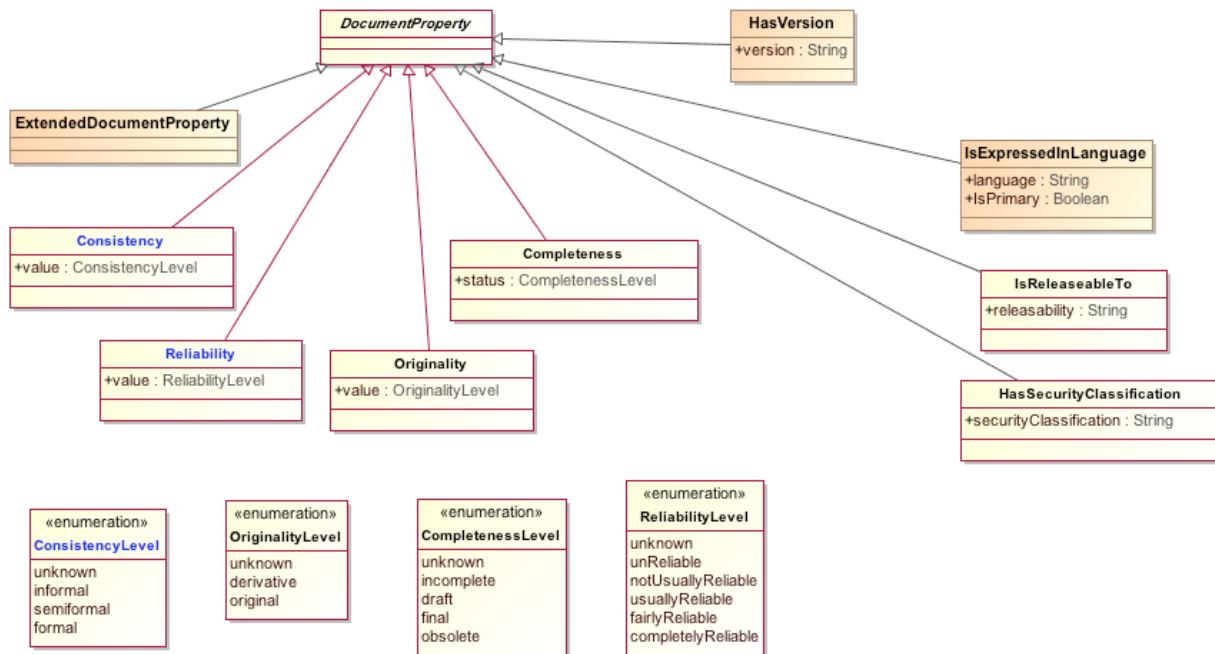


Figure 11.2 - Document Properties class diagram

defines various statements related to

11.2.1 Document Property (abstract)

This class defines characteristics of documents. Other characteristics common to all Exhibits are defined using ExhibitProperty. Each concrete subclass of DocumentProperty defines a certain statement that describes a characteristic of document. The subject of the statement is the instance of Document that owns the DocumentProperty element. The DocumentProperty statement is formed by combining the owning Document with the objects into the sentential form determined by the concrete subclass of the DocumentProperty element. See subsequent sections for detail.

~~Each concrete subclass of DocumentProperty defines a single characteristic of the document. An instance of a concrete subclass of the DocumentProperty class that is owned by some Document object defines a characteristic of the document represented by the Document object.~~

11.2.2 HasVersion

It is often important to identify a particular version of the document. DocumentProperty HasVersion shall be used for this purpose.

statement shall

Superclass

DocumentProperty

Attributes

- version:String
Designator of the version of the original Document.

Semantics

HasVersion element represents a property of the owner Document object that identifies the version of the original document. The version property establishes a relationship between the owner Document object and the designation of the version of the original document. The ElectronicSource is a snapshot of the original document captured in electronic form. The version is used to provide full traceability to the original document.

Document has version version

The main characteristic is expressed by a sentential form “Document has version.”

11.2.3 IsExpressedInLanguage

The use of language is one of the essential characteristics of a document. The meaning of the document is expressed as a text that uses a certain vocabulary that is expressed in some language. In the context of the Evidence Metamodel, IsExpressedInLanguage is a document property that established relationship between a document and the language which is essential to understanding the meaning of the document. The language itself is identified as a string attribute of the Language property.

statement identifies

described by

Superclass

DocumentProperty

Attributes

- language:String
Designation of the language which is used in the owner Document.
- IsPrimary:Boolean
In case when the document is expressed in multiple languages, this attribute identifies the primary language.

Constraints

- Document should have at least one IsExpressedInLanguage property.
- In case when the Document is expressed in more that one language, the IsPrimary property may be used to identify the primary language.

Semantics

IsExpressedInLanguage element represents a property of the owner Document object that identifies the language of the document. The source property establishes a relationship between the owner Document object and the designation of the language, which is interpreted as the name of a language. A language can be a natural language or an unnatural one, such as a computer language, a system of mathematical symbols, or a modeling notation. ISO-639-2 provides manes of many languages and provides short language-independent codes. In the scope of the Evidence Metamodel, the language of each document shall be identified, as this is vital to interpretation of evidence and for exchanging evidence. It is possible that a Document is expressed in more than one language. The SACM Evidence Metamodel allows identifying the primary language by setting the isPrimary attribute to true.

The main characteristic is expressed by a sentential form “Document is expressed in language.” Additional sentential form is “Document is primarily expressed in language.”

The statement

11.2.4 HasSecurityClassification

In some contexts of evidence evaluation it is required to track the security classification of documents. Evidence management tools can use security classification in filters in order to protect sensitive information.

HasSecurityClassification **property represents** security classification of the owner Document.

Superclass

DocumentProperty

statement identifies

Attributes

- securityClassification:String
Designation of the security classification of the owner document.

Semantics

statement

HasSecurityClassification **element represents a property of the owner Document object that** identifies the security classification of the original document. **The SecurityClassification property establishes a relationship between the owner Document object and the designation of the security property of the original document.** SecurityClassification property of the owner Document refers also to all ElectronicSource of the Document. Examples of designations of security classifications are: “Unclassified,” “Secret,” “Top Secret.” When the HasSecurityClassification property is omitted, the Document is assumed to be “Unclassified.”

Document has security classification security classification

The main characteristic is expressed by a sentential form “Document has security classification.”

11.2.5 IsReleasableTo

The statement

In some contexts of evidence evaluation it is required to track of the releasability of documents. Evidence management tools can use releasability property in filters in order to protect sensitive information. IsReleasableTo **property represents security classification** of the owner Document.

Superclass

DocumentProperty

releasability

statement identifies

Attributes

- releasability:String
Designation of the releasability of a document.

Semantics

statement

IsReleasableTo **element represents a property of the owner Document object that** identifies the releasability of the original document. **The IsReleasableTo property establishes a relationship between the owner Document object and the designation of the releasability scope of the original document.** IsReleasableTo property of the owner Document refers also to all ElectronicSource of the Document. Examples of designations of releasability scope are: “US eyes only,” “Canadian eyes only,” “NATO only.” When the IsReleasableTo property is omitted, the Document is assumed not to have releasability restrictions.

The main characteristic is expressed by a sentential form “Document is releasable to releasability scope.”

The statement

Example

11.2.6 Originality statement

Originality ~~element represents characteristic of documents that~~ is asserted during the course of evaluation and ~~that~~ refers to the originality of the document. This characteristic refers to the document (record) that is the source of evidence. The original source is one that contributes written, oral, or visual information not derived from a prior written or visual record or oral communication. A derivative source is one that contributes information that was copied, transcribed, abstracted, summarized, duplicated, or repeated from information is a previously existing source (that is from the original or another derivative).

Superclass

DocumentAttribute

Attributes

- value:OriginalityLevel
Originality level, such as derivative or original.

The statement of Originality is verbalized as follows:

- Document is Original
- Document is Derivative
- Originality of Document is unknown

11.2.7 OriginalityLevel (enumeration)

OriginalityLevel enumeration class defines the Originality levels.

Literals

- unknown
Originality level is unknown.
- derivative
Document is derivative.
- original
Document is original.

11.2.8 Consistency statement

Consistency ~~element represents characteristic of documents that~~ is asserted during the course of evaluation and ~~that~~ refers to the consistency of the document. This characteristic refers to the level of formality of the document and to our capability to interpret the document. Consistency of a document can be informal, semi-formal, and formal. An informal document uses prose. A semi-formal document uses a template that determines some of its structure, filled in by prose. A form with a large amount of prose is an example of a semi-formal document. When the amount of prose becomes limited, the document may be referred to as formal. A multiple-choice questionnaire is an example of a formal document.

Superclass

DocumentAttribute

Attributes

- value:ConsistencyLevel
Consistency level of the Document, such as informal, semi-formal, and formal.

The statement of Consistency is verbalized as follows:

- Document is formal
- Document is semi-formal
- Document is informal
- Consistency of Document is unknown

11.2.9 ConsistencyLevel (enumeration)

The ConsistencyLevel enumeration class defines consistency levels.

Literals

- unknown
Consistency level is unknown
- informal
Consistency level is informal
- semiformal
Consistency level is semi-format
- formal
Consistency level is formal

11.2.10 Completeness statement

Completeness ~~element represents a characteristic of documents that~~ is asserted during the course of evaluation and ~~that~~ refers to the completeness of the document. This characteristic refers to the point in the lifecycle of the current version of the document and to our capability to derive useful information from the document. Completeness of a document can be incomplete, draft, final, and obsolete. An incomplete document may not be reliable and may contain omissions. A draft document is more reliable and is likely not to contain omissions. A final document is the most reliable state. When the document is obsolete, it may not be a source of high-fidelity information. Evidentiary support from documents that are not final may be contested. Completeness level can be applied to Evidence package.

Superclass

DocumentAttribute

Attributes

- value:CompletenessLevel
Completeness level, such as incomplete, draft, final, and obsolete.

11.2.11 CompletenessLevel (enumeration)

The CompletenessLevel enumeration class defines completeness levels.

Literals

- unknown
Completeness level is unknown.
- incomplete
The subject is incomplete.
- draft
The subject is a draft.
- final
The subject is final.
- obsolete
The subject is obsolete.

The statement of Completeness is verbalized as follows:

- Document is final
- Document is draft
- Document is incomplete
- Document is obsolete
- The completeness of Document is unknown

11.2.12Reliability

statement

Reliability ~~element represents a characteristic of documents that~~ is asserted during the course of evaluation and ~~that~~ refers to the reliability of the source of the information contained in the document. This characteristic refers to the level of trust the evaluator confers to the source of the document and therefore to the document itself. Reliability of the document affects the strength of evidentiary support this document provides. The Evidence Metamodel defines 5 levels of reliability.

Superclass

EvidenceAttribute

Attributes

- value:ReliabilityLevel
Level of reliability of the Document, such as unreliable, not usually reliable, usually reliable, fairly reliable, completely reliable.

11.2.13ReliabilityLevel (enumeration)

The ReliabilityLevel enumeration class defines reliability levels.

Literals

- unknown
Reliability level is unknown.
- unReliable
The source is unreliable.
- nonUsuallyReliable
The source often unreliable.
- usuallyReliable
The source usually reliable.
- fairlyReliable
The source is fairly reliable.
- completelyReliable
The source is completely reliable.

The statement of Reliability is verbalized as follows:

- Document is from a completely reliable source
- Document is from a fairly reliable source
- Document is from a usually reliable source
- Document is from an often unreliable source
- Document is from an unreliable source
- Reliability of the document is unknown

11.2.14ExtendedDocumentProperty

ExtendedDocumentProperty element represents a user-defined characteristic of a document that is asserted during the course of evaluation.

Superclass

DocumentProperty

Constraints

ExtendedDocumentProperty element shall own at least one TaggedValue describing the meaning of the element.

Associations

- `role:RoleBinding[0..*]`
Set of role bindings that further describe which FormalObjects are bound to the roles that are determined by the fact type.
- `definition:MOF::Element`
A link to an entry of an external SBVR vocabulary or an OWL ontology defining the fact type of the assertion.

Semantics

Assertion is an element of meaning that states existence of a relationship between several individual formal objects. In a formal assurance case, the nature of the relationship is specified through a reference to an external vocabulary, such as an SBVR vocabulary or an OWL ontology. SACM assumes that community of interest for an assurance case will acquire or develop such vocabularies for the corresponding subject area. In a semi-formal assurance case the nature of the relationship can be described informally through a 'content' property. In this case the 'definition' property and the 'facttype' property shall not be used. However the references to the exact FormalObjects through RoleBinding elements still can be stated. The 'content' property of the FormalAssertion element provides the verbalization of the assertion, which is the expression of the assertion in the selected natural language. For informal assurance cases, a ReferencedClaim element can be used, which only contains the verbalization of the claim in a natural language.

12.3.2 ReferencedClaim

ReferencedClaim is an element of meaning that represents an informal assertion about the state of affairs in the subject area about which an assurance case is developed. ReferencedClaim can be linked to a Claim element of the Argumentation part of an assurance case.

Superclass

FormalAssertion

Associations

- `claim:Argumentation::Claim[0..1]`
A link to a Claim element in the Argumentation part of an assurance case (if available).

Semantics

└ makes

ReferencedClaim is an element of meaning that **states** an assertion about a subject area of an assurance case. ReferencedClaim represents the claim as prose in a selected natural language (formal or informal), without identifying its structure. ReferencedClaim element can represent informal claims (claims not linked to any formal definition of its meaning, such as an ontology developed by some community of meaning) or unstructured claims (where the subjects are not identified).

Usually claims assert existence of a formally defined relationship between several individual subjects and involve several objects bound to specific roles. An Assertion element can be used to capture this structure of a claim in a more formal way. In particular, Assertion element can link the proposition to an external vocabulary or ontology that defines the exact meaning of the proposition, as well as the exact subjects of the proposition.

12.3.3 RoleBinding

A claim usually states existence of a relationship between several individual domain objects and involves several subjects bound to specific roles. RoleBinding element is used to capture this structure of a claim in a more formal way in the context of an Assurance element representing the claim.

Superclass

UtilityElement

Attributes

- role:String
Name of the Role in the fact type to which an object is bound.

Associations

- subject:FormalObject[0..1]
FormalObject that is bound to this Role.

Semantics

— instance

RoleBinding **object** is owned by an Assertion object that provides the context, including the definitions of roles and the types of domain objects that can be bound to each role. The formal definition of the relationship represented by an Assertion element is provided by a reference to an external ontology, which can be either an SBVR vocabulary or an OWL ontology. This definition shall at a minimum include the definition of roles, to which the RoleBinding elements shall conform. In particular, the ‘role’ attribute of a RoleBinding shall correspond to a particular role in the formal definition of a relationship. Further, for each role contained in the formal definition of the relationship there shall be exactly one RoleBinding element, in which the ‘role’ attribute matches the name of the role and the subject matches the allowed type of subject for that role.

SACM allows incremental construction of the conceptual model underlying an assurance case, therefore it allows temporarily unbound roles. A completed Body of Evidence accompanying an Assurance Case shall meet the condition that all RoleBinding elements have the corresponding subject of appropriate type.

— asserts

SACM provides a built-in relation “IsA” between any EvidenceElement and an Object, which **states** the definition of an EvidenceItem. This mechanism can be used to build the entire formal vocabulary inside the Evidence Model, where the external references can be reduced to a mere handful of meta-meta level concepts (in the extreme case, the only external reference that is needed is the concept “thing,” other definitions can, at least in principle, be provided through the “IsA” relationships internal to the Evidence Model. This approach can be used when the external formal vocabulary is not available, and there is a need to use more unified tooling environment.

From the formal logic perspective, SACM distinguishes objects from assertions. As a consequence, in order to represent a formal assertion about other assertions the later must be objectified, i.e., represented as a FormalObject that refers to the original assertion using the element ObjectifiedAssertion.

13 Evidence Properties

13.1 General

Property statements identify various custody, Evidence Properties defines provenance and timing characteristics of the evidence items and evaluations.

13.2 Custody Class Diagram

The Custody Class Diagram represents various statements related to the Custody of an EvidenceElement. These statements describe the custodians of an evidence element, the locations associated with various events in the lifecycle of the evidence element, as well as the process by which the element was obtained.

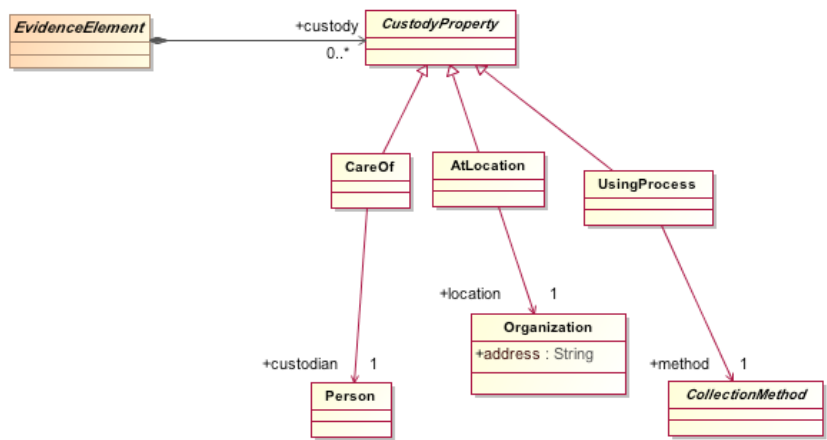


Figure 13.1 - Custody class diagram

13.2.1 CustodyProperty (abstract)

various statements related to the custody of an evidence element statements

CustodyProperty is an abstract class that represents a custody property of an evidence event. Concrete custody properties are defined by subclasses of CustodyProperty.

Superclass Each concrete subclass of CustodyProperty defines a certain statement that describes a characteristic of an evidence element. The subject of the statement is the instance of EvidenceElement that owns the CustodyProperty element.
Semantics The CustodyProperty statement is formed by combining the owning EvidenceElement with the objects into the sentential form determined by the concrete subclass of the CustodyProperty element. See subsequent sections for detail.

CustodyProperty element represents a property of the owner EvidenceEvent object. CustodyProperty element is an abstract class that establishes a relationship between the owner evidence event object and the particular custody property, defined by a particular concrete subclass of the CustodyProperty element and further interpreted by the context of a particular event (as described by a property meaning table of a particular evidence event).

13.2.2 CareOf

statement identifies subject

CareOf is a characteristic of an EvidenceEvent that specifies the custodian of the associated evidence element.

Superclass

CustodyProperty

Associations

- `custodian:Person[1]`
Custodian of the evidence element associated with the subject **EvidenceEvent**.

(EvidenceElement

Semantics

statement asserts

CareOf ~~element represents a property of the subject EvidenceEvent and its associated EvidenceElement. CareOf element represents~~ the state of affairs that the person identified in the 'custodian' attribute of the CareOf object is the custodian of the owner EvidenceElement object ~~(with the additional constraints imposed by the semantics of the owned EvidenceEvent).~~

13.2.3 AtLocation

statement identifies

subject

AtLocation ~~is a characteristic of an EvidenceEvent that specifies~~ the location of the ~~associated~~ evidence element.

Superclass

CustodyProperty

Associations

- `location:Organization[1]`
Location of the evidence event or the associated owner EvidenceElement.

Semantics

statement asserts

AtLocation ~~element represents a property of the owner EvidenceEvent and its associated EvidenceElement. AtLocation element represents~~ the state of affairs that the location identified in location attribute of the AtLocation object is the location of the owner EvidenceElement object ~~(with the additional constraints imposed by the semantics of the owned EvidenceEvent).~~

13.2.4 UsingProcess

statement identifies

UsingProcess ~~is a characteristic of an EvidenceEvent that specifies~~ the method by which the event was performed.

Superclass

CustodyProperty

Associations

- `method:CollectionMethod[1]`
CollectionMethod involved at the owner **EvidenceEvent**

EvidenceElement

Semantics

statement asserts

UsingProcess ~~element represents a property of the owner EvidenceEvent. UsingProcess element represents~~ the state of affairs that the CollectionMethod identified in method attribute of the UsingProcess object is the method involved at the owner **EvidenceEvent** object ~~(with the additional constraints imposed by the semantics of the owned EvidenceEvent).~~

EvidenceElement

13.3 EvidenceEvents Class Diagram

The EvidenceEvents Class Diagram describes evidence statements related to the Events that determine the lifecycle of an evidence element. EvidenceEvents set the context for additional timing, provenance, and custody **properties** associated with the subject evidence element. Therefore EvidenceEvents allow representing the entire Chain of Custody of the evidence element. EvidenceEvents statements are owned by the subject evidence element.

statements (or clauses)

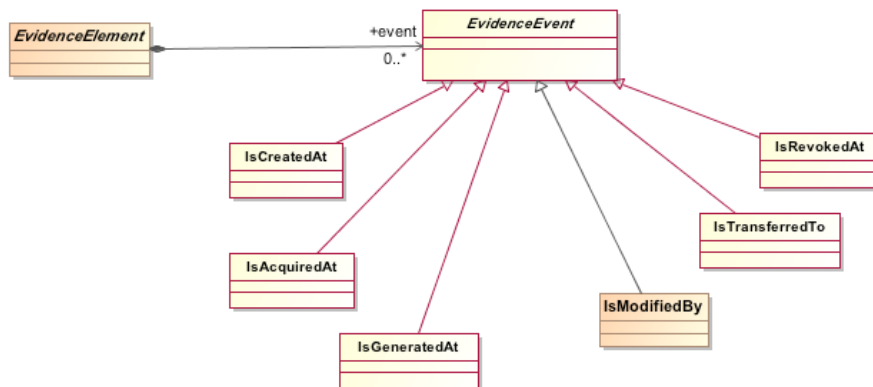


Figure 13.2 - EvidenceEvent Class Diagram

13.3.1 EvidenceEvent (abstract)

EvidenceEvent represents statements related to the events in the lifecycle of an evidence element. The lifecycle of an evidence element is determined by several events, such as Creation, Acquisition, or Derivation of the evidence element; Transfer of the evidence element; Modification of the evidence element; Evaluation of the evidence element; and Revocation of the evidence element. Semantics of concrete evidence events is defined for the subclasses of EvidenceEvent element. An EvidenceEvent statement describes a certain characteristic of the subject evidence element. More complex Event statements can be constructed by adding further Timing, Provenance, and Custody clauses to EvidenceEvents of the subject evidence element. In particular, the mechanism of EvidenceEvents allows making statements about the time-dependent characteristics of the subject evidence element, since each EvidenceEvent can be the subject of its own timing clause. The entire chain of custody of an evidence element can be established by analyzing the EvidenceEvents of the element. On the other hand, the Timing, Provenance, and Custody clauses of the subject evidence element itself (EvidenceProperty objects that are directly owned by the EvidenceElement object) state essential characteristics of the EvidenceElement that do not change over time.

Statements about evidence elements can be revoked and updated statements can be made. The ModifiedBy event statement can be used to provide record of the modification elements.

Superclass

EvidenceProperty

Semantics

EvidenceEvent represents statements related to the lifecycle events of the subject EvidenceItem. Further detail of the event are provided by the EvidenceProperty elements owned by the EvidenceEvent. The set of EvidenceEvent owned by an EvidenceItem establishes the chain of custody for the EvidenceItem.

The EvidenceEvent element is an abstract class that establishes a relationship between the subject evidence item and the particular event description with its associated characteristics, defined by a particular concrete subclass of the EvidenceEvent element and its owned properties, such as CustodyProperty, Provenance, and TimingProperty.

13.3.2 IsAcquiredAt

IsAcquiredAt is an Evidence Event that describes an acquisition of an evidence element and thus initiates the lifecycle of the evidence element. Other evidence events that initiate the lifecycle of evidence element are creation of an evidence element and generation of an evidence element. Acquisition emphasizes an event at which custody is established over a pre-existing item.

Superclass

EvidenceEvent

Semantics

event statement asserts

IsAcquiredAt element represents a property of the owner EvidenceElement object. IsAcquiredAt element represents the state of affairs that the owner object is acquired. IsAcquiredAt may own further properties establishing additional details about the acquisition event.

Clause

clauses

Property	Meaning	Verbalization
AtTime	Time of the acquisition	Element <i>is acquired at</i> time
EffectiveTime	N/A	
CreatedBy	N/A	
PerformedBy	The stakeholder who acquired the evidence element	Element <i>is acquired by</i> stakeholder
ApprovedBy	The person or organization who approved the acquisition.	<i>Acquisition of</i> element <i>is approved by</i> stakeholder
OwnedBy	Organization which executed acquisition of the evidence element and has custody of the evidence element.	Element <i>is owned by</i> stakeholder
CareOf	The custodian of the evidence element within the owner organization.	Person <i>is custodian of</i> element
AtLocation	The location of the evidence document at which it was acquired.	Element <i>is acquired at</i> location
UsingProcess	The reference to a CollectionMethod object that provides a definition of the process involved in the acquisition.	Element <i>is acquired using</i> method

13.3.3 IsCreatedAt

Multiple clauses can be combined into compound statements, for example, "Person *became custodian of* element *at* time"

IsCreatedAt is an Evidence Event that describes creation of an evidence element and thus initiates the lifecycle of the evidence element. Other evidence events that initiate the lifecycle of evidence element are acquisition of an evidence element and generation of an evidence element. Creation emphasizes an event by which a primary evidence item comes to existence. Generation emphasizes event by which a secondary (derived) evidence element comes to existence.

Superclass

EvidenceEvent

Semantics

event statement asserts

IsCreatedAt ~~element represents a property of the owner EvidenceElement object.~~ IsCreatedAt element represents the state of affairs that the owner object is created. This usually applied to primary evidence elements. IsCreatedAt may own further ~~properties~~ establishing additional details about the creation event.

Clause  clauses

Property	Meaning	Verbalization
AtTime	Time of creation	Element <i>is created at</i> time
EffectiveTime	Effective time of the evidence element	
CreatedBy	N/A	
PerformedBy	The source of the evidence element	Element <i>is created by</i> stakeholder
ApprovedBy	The person or organization who approved the creation of the evidence element.	<i>Creation of</i> element <i>is approved by</i> stakeholder
OwnedBy	Organization which created the evidence element.	Element <i>is owned by</i> stakeholder
CareOf	The custodian of the evidence element within the owner organization.	Person <i>is custodian of</i> element
AtLocation	The location of the evidence document at which it was created; this location may be different from the location of the organization that created the event.	Element <i>is created at</i> location
UsingProcess	The reference to a CollectionMethod object that provides a definition of the process involved in the creation of the document.	Element <i>is created using</i> method

13.3.4 IsTransferredTo

Multiple clauses can be combined into compound statements, for example, "Element was created by stakeholder at time using method"

IsTransferredTo is an Evidence Event that describes a transfer of an already established evidence element and thus continues the lifecycle of the evidence element. Transfer emphasized change of custody.


Superclass

EvidenceEvent

Semantics

event statement asserts

IsTransferredTo ~~element represents a property of the owner EvidenceElement object.~~ IsTransferredTo element represents the state of affairs that the owner object is transferred to a different custody. IsTransferredTo element may own further ~~properties~~ establishing additional details about the transfer event.

clauses 

Multiple clauses can be combined into compound statements, for example, "Element was transferred to location at time by stakeholder"

Clause

Property	Meaning	Verbalization
AtTime	Time of the transfer	Element <i>is transferred at</i> time
EffectiveTime	N/A	
CreatedBy	N/A	
PerformedBy	The stakeholder who transferred the evidence element	Element <i>is transferred by</i> stakeholder
ApprovedBy	The person or organization who approved the transfer of the evidence element.	<i>Transfer of</i> element <i>is approved by</i> stakeholder
OwnedBy	Organization which established custody over the evidence element.	Element <i>is owned by</i> stakeholder
CareOf	The custodian of the evidence element.	Person <i>is custodian of</i> element
AtLocation	The new location of the evidence document after the transfer; this location may be the same as the location of the organization that took custody of the document, however these two locations may be different.	Element <i>is transferred to</i> location
UsingProcess	The reference to a CollectionMethod object that provides a definition of the process involved in the transfer of the document.	Element <i>is transferred using</i> method

13.3.5 IsModifiedBy

IsModifiedBy is an Evidence Event that describes a modification of an evidence element throughout its lifecycle. Modification event emphasizes changes to the original exhibit or changes in the meaning of the FormalAssertion or EvidenceAssertion, or changes to the ProjectElement. The IsModifiedBy element can be the subject of additional Timing, Provenance, and Custody clauses.

Superclass

EvidenceEvent

Semantics

event statement asserts

IsModifiedBy ~~element represents a unique modification event throughout its lifecycle of the subject EvidenceElement object.~~ IsModifiedBy element represents the state of affairs that the owner object is modified. IsModifiedBy may include additional clauses that provide further details about the modification event. In particular, an Annotation clause can be used to describe the nature of the modification.

Clause

Property	Meaning	Verbalization
AtTime	Time of the modification	Element <i>is modified at</i> time
EffectiveTime	N/A	
CreatedBy	N/A	
PerformedBy	The stakeholder who modified the evidence element	Element <i>is modified by</i> stakeholder
ApprovedBy	The stakeholder who approved the modification of the evidence element.	<i>Modification of</i> element <i>is approved by</i> stakeholder
OwnedBy	N/A	
CareOf	The custodian of the evidence element.	Person <i>is custodian of</i> element
AtLocation	The location oat which the modification of the evidence element is performed	Element <i>is modified at</i> location
UsingProcess	The reference to a method by which the evidence element is modified	Element <i>is modified using</i> method

13.3.6 IsRevokedAt

IsRevokedAt is an Evidence Event that describes revocation of an already established evidence element and thus describes the end of the lifecycle of the evidence element. Revocation of an evidence document means that the evidence element is no longer admissible for supporting arguments while it is still available e.g., as an item in an evidence repository. A revoked element may still remain as the subject of assertions stating evidentiary support to some claims. Such relations may need to be evaluated and explicitly negated based on the revocation event. Revocation of an evidence element is stronger than the end of the validation period of an evidence element.

Superclass

EvidenceEvent

Semantics

event statement asserts

IsRevokedAt ~~element represents a property of the subject EvidenceElement object. IsRevokedAt element represents~~ the state of affairs that the subject has been revoked. IsRevokedAt element may be the subject of additional properties describing further details about the revocation event.

Clause

Property	Meaning	Verbalization
AtTime	Time of the revocation	Element <i>is revoked at</i> time
EffectiveTime	N/A	
CreatedBy		
PerformedBy	The stakeholder who revoked the evidence element	Element <i>is revoked by</i> stakeholder
ApprovedBy	The person or organization who approved the revocation of the evidence element.	<i>Revocation of</i> element <i>is approved by</i> stakeholder
OwnedBy	Organization which established custody over the evidence element, if applicable.	Element <i>is owned by</i> stakeholder
CareOf	The custodian of the evidence element.	Person <i>is custodian of</i> element
AtLocation	N/A	
UsingProcess	The reference to a CollectionMethod object that provides a definition of the process involved in the revocation of the document.	Element <i>is revoked using</i> method

13.3.7 IsGeneratedAt

IsGeneratedAt is an Evidence Event that describes generation of a derived evidence element and thus initiates the lifecycle of the evidence element. Other evidence events that initiate the lifecycle of evidence element are acquisition of an evidence element and creation of an evidence element. Creation emphasizes an event by which a primary evidence item comes to existence. Generation emphasizes event by which a secondary (derived) evidence element comes to existence. Acquisition emphasizes taking custody of a pre-existing item.

Superclass

EvidenceEvent

Semantics

event statement asserts

IsGeneratedAt ~~element represents a property of the owner EvidenceElement object. IsGeneratedAt element represents~~ the state of affairs that the owner object is generated. This usually applies to primary evidence elements. IsGeneratedAt may own further ~~properties~~ establishing additional details about the creation event.

clauses



Clause

Property	Meaning	Verbalization
AtTime	Time of generation	Element <i>is generated at</i> time
EffectiveTime	Effective time of the generated evidence element	
CreatedBy	N/A	
PerformedBy	The stakeholder who generated the evidence element	Element <i>is generated by</i> stakeholder
ApprovedBy	The person or organization who approved the generation of the evidence element.	<i>Generation of</i> element <i>is approved by</i> stakeholder
OwnedBy	Organization which executed generation of the evidence element.	Element <i>is owned by</i> stakeholder
CareOf	The custodian of the evidence element within the owner organization.	Person <i>is custodian of</i> element
AtLocation	The location of the evidence document at which it was generated.	Element <i>is generated at</i> location
UsingProcess	The reference to a CollectionMethod object that provides a definition of the process involved in the generation of the document.	Element <i>is transferred using</i> method

13.4 Provenance Class Diagram

statements (or clauses to other statements)

The Provenance Class Diagram focuses on the Provenance characteristics: who create the evidence element, or who evaluated it, who approved it, and what organization owns the evidence element.

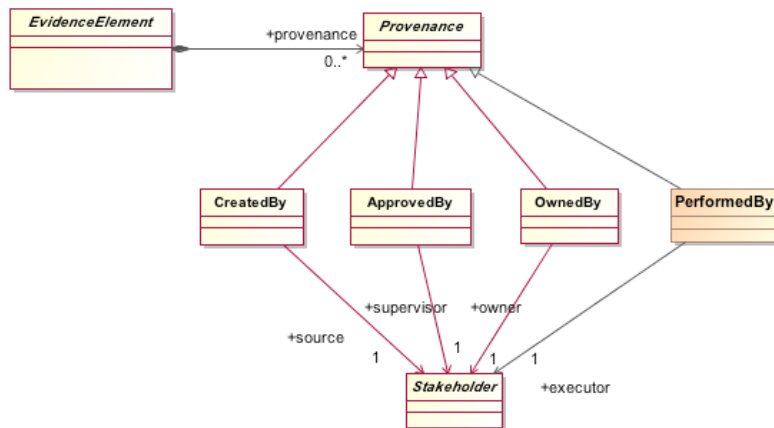


Figure 13.3 - Provenance Class Diagram

various statements related to the provenance of the subject evidence element. Concrete statements are defined by the subclasses of Provenance element.

13.4.1 Provenance (abstract)

Provenance element is an abstract class that represents any provenance characteristic. In the SACM Evidence Metamodel this element is utilized to specify which elements can have provenance properties. Specific provenance characteristics extend Provenance element.

Superclass

EvidenceProperty

Semantics

Provenance element represents a property of the owner EvidenceElement object or EvidenceAttribute object. This element is an abstract class that establishes a relationship between the owner object and the particular provenance characteristic, defined by a particular concrete subclass of the Provenance element.

13.4.2 CreatedBy

statement identifies

CreatedBy element represents the source of the owner object. The source can be a person or an organization, collectively referred to as a stakeholder.

Superclass

Provenance

Each concrete subclass of Provenance defines a certain statement that describes a characteristic of an evidence element. The subject of the statement is the instance of EvidenceElement that owns the Provenance element. The Provenance statement is formed by combining the owning EvidenceElement with the objects into the sentential form determined by the concrete subclass of the Provenance element. See subsequent sections for detail.

Associations

- source:Stakeholder[1]
The source of the owner object.

Semantics

statement asserts

CreatedBy element represents a property of the owner EvidenceElement object or EvidenceAttribute object. CreatedBy element represents the state of affairs that the owner object was created by the particular stakeholder, defined by stakeholder object. Stakeholder of an evidence object can be a person or an organization.

The characteristic of CreatedBy is expressed by a sentential form "Element is created by stakeholder."

13.4.3 ApprovedBy

statement

ApprovedBy element represents the supervisor of the owner object. The supervisor can be a person or an organization, collectively referred to as a stakeholder.

Superclass

Provenance

statement identifies

Associations

- supervisor:Stakeholder[1]
The supervisor of the owner object.

Semantics

statement asserts

ApprovedBy ~~element represents a property of the owner EvidenceElement object or EvidenceAttribute object.~~

ApprovedBy ~~element represents~~ the state of affairs that the owner object has been approved by the particular stakeholder, defined by stakeholder object. Stakeholder of an evidence object can be a person or an organization.

The ~~characteristic~~ of ApprovedBy is expressed by a sentential form "Element is approved by stakeholder."

13.4.4 OwnedBy

statement

OwnedBy ~~element represents~~ the owner of the evidence object. The owner can be a person or an organization, collectively referred to as a stakeholder, however in practice, the owner is usually an organization.

Superclass

statement identifies

Provenance

Associations

- owner:Stakeholder[1]
The owner of the evidence object.

Semantics

statement asserts

OwnedBy ~~element represents a property of the owner EvidenceElement object or EvidenceAttribute object. OwnedBy~~

~~element represents~~ the state of affairs that the owner object (which is the technical term referring to the fact that the OwnedBy property is owned by some object of EvidenceElement or EvidenceAttribute class) is owned by the particular subject, defined by Stakeholder object. Stakeholder of an evidence object can be a person or an organization.

The ~~characteristic~~ of OwnedBy is expressed by a sentential form "Element is owned by stakeholder."

13.4.5 PerformedBy

statement

PerformedBy ~~element represents the provenance clause that states~~ the stakeholder who executes an evidence object. The clause can refer to a person or an organization, collectively referred to as a stakeholder.

Superclass

statement identifies

Provenance

Associations

- executor:Stakeholder[1]
The executor of the evidence event.

Semantics

statement asserts

PerformedBy ~~element represents a clause of an evidence statement related to the subject EvidenceElement. PerformedBy~~

~~element represents~~ the state of affairs that the subject event is executed by the particular stakeholder, defined by 'executor' object. Executor of an evidence event can be a person or an organization.

The ~~characteristic~~ of PerformedBy is expressed by a sentential form "Event is performed by executor."

statement

13.5 Timing Class Diagram

statements (or clauses of other statements)

The Timing Class Diagram focuses at the Timing characteristics: when the evidence element was created, what is its effective date, and until when it is valid.

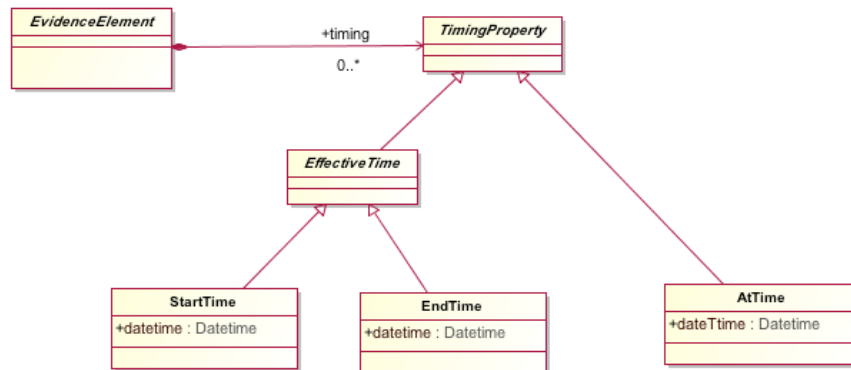


Figure 13.4 - Timing Class Diagram

13.5.1 TimingProperty (abstract)

various statements related to the timing of the subject evidence element. Concrete statements are defined by the subclasses of TimingProperty element.

TimingProperty element is an abstract class that represents any timing characteristic. In the SACM Evidence Metamodel this element is utilized to specify which elements can have timing properties. Specific timing characteristics extend TimingProperty element.

Superclass

EvidenceProperty

Semantics

Each concrete subclass of TimingProperty defines a certain statement that describes a characteristic of an evidence element. The subject of the statement is the instance of EvidenceElement that owns the TimingProperty element. The TimingProperty statement is formed by combining the owning EvidenceElement with the objects into the sentential form determined by the concrete subclass of the TimingProperty element. See subsequent sections for detail.

TimingProperty element represents a property of the owner EvidenceElement object or EvidenceAttribute object. This element is an abstract class that establishes a relationship between the owner object and the particular timing characteristic, defined by a particular concrete subclass of the TimingProperty element.

13.5.2 EffectiveTime (abstract)

EffectiveTime element represents various compound statements that involve a certain time interval during which a certain proposition is asserted to be true (time-dependent assertions involving an “effective” time period). Specific characteristics related to the effective time interval are defined by concrete subclasses of EffectiveTime element.

Superclass

TimingProperty

Semantics

statement asserts

EffectiveTime element represents a statement about the owner EvidenceElement (an object that owns the instance of one of the concrete subclasses of this element). The EffectiveTime element specifies a time interval associated with the subject, during which the subject is asserted to be “effective.” For example, in case of an EvidenceAssertion or a FormalAssertion, this element specifies a time interval at which the corresponding statement is asserted to be true. In case of an EvidenceItem this element specifies the relevant time context in which the element shall be considered.

13.5.3 StartTime

statement asserts

This element represents the start of the effective time interval of the owner evidence object.

Superclass

StartTime statement identifies

EffectiveTime

Attributes

- datetime:EDate[1]
Date starting from which the owner object becomes valid.

Constraints

- One object shall not own more than one StartTime property.
- When object owns StartTime and EndTime, the datetime of the StartTime property shall be earlier than or equal to the datetime of the EndTime property.

Semantics

statement asserts

StartTime element represents a property of the owner EvidenceElement object or EvidenceAttribute object. StartTime element represents the state of affairs that the owner object is valid starting from the datetime stated by the StartTime property.

13.5.4 EndTime

EndTime statement identifies

This element represents the end of the effective time interval of the owner evidence object.

Superclass

EffectiveTime

Attributes

- datetime:EDate[1]
Date after which the owner object ceases to be valid.

Constraints

- One object shall not own more than one EndTime property.
- When object owns StartTime and EndTime, the datetime of the EndTime property shall be later than or equal to the datetime of the StartTime property.

Semantics

statement asserts

EndTime ~~element represents a property of the owner EvidenceElement object or EvidenceAttribute object. EndTime element represents~~ the state of affairs that the owner object is not valid after from the datetime stated by the EndTime property.

13.5.5 AtTime

~~This element represents~~ the time stamp for the owner evidence object. The context for the timestamp is given by the owner object.

AtTime statement identifies

Superclass

TimingProperty

Attributes

- datetime:EDate[1]
The timestamp associated with the owner object.

Semantics

statement asserts

AtTime ~~element represents a property of the owner EvidenceElement object or EvidenceAttribute object. AtTime element represents~~ the state of affairs that involves an association between the owner object and the datetime stated by the AtTime property.

14 Evidence Evaluation

14.1 General

Evaluation of Evidence involves making certain assertions about evidence items and their relations to the subject area claims. Evidence Assertions are defined within the Evidence Metamodel and include the following categories:

- Properties of Documents as they are related to the quality of the evidentiary support that may be offered by these documents, such as Primary or secondary document, original or derived document, Consistency, Completeness, Accuracy of the document. These properties are independent on an assurance case for which the evidence is collected.
- Attributes of the evidentiary support, such as Direct or indirect, Relevance, Confidence, Strength, and Significance.
- Interpretation of Evidence: what an evidence item “Is” what it “means.”
- Nature of evidentiary support: Supports, Challenges.
- Observations and Resolutions.
- Standard of Proof to which evidence is evaluated.

14.2 Evidence Relations Class Diagram

The Evidence Relations Class Diagram provides elements that represent statements of evidentiary support relations between an EvidenceItem, such as an Exhibit and a FormalAssertion.

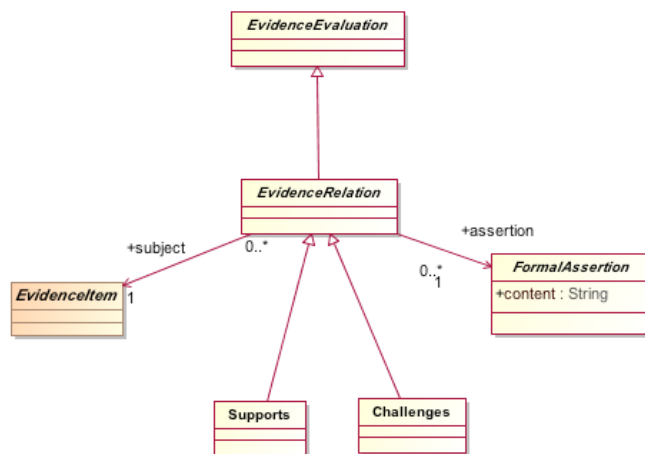


Figure 14.1 - EvidenceRelations Class Diagram

14.2.1 EvidenceRelation (abstract)

EvidenceRelation is an abstract class that represents an evidence relation between one EvidenceItem and one FormalAssertion element. Concrete nature of these relations is defined by the subclasses of the EvidenceRelation element.



Abstract class EvidenceEvaluation has been introduced earlier in section 10.2 EvidenceAssertions during the overview of the Evidence Metamodel. Instances of EvidenceRelation are owned directly by EvidenceContainer (see section 15 Administration)

various statements of evidentiary support

Superclass

EvidenceEvaluation

Associations

- subject:EvidenceItem[1] 
The EvidenceItem **object**, such as an Exhibit or a Document that is the subject of an evidentiary **relation** to a FormalAssertion object such as a ReferencedClaim. 
- assertion:FormalAssertion[1]
FormalAssertion **object** that receives an evidentiary **relation** from the EvidenceItem object.

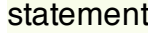
Constraints

- FormalAssertion shall not receive evidence relation from self.

Semantics

EvidenceRelation is a unit of information generated during evidence evaluation. It represents a relationship between an EvidenceItem and FormalAssertion objects that is asserted during the evidence evaluation.

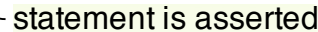
14.2.2 Supports

Supports **element**  represents an evidence relation between one EvidenceItem and one FormalAssertion element where the EvidenceItem confers evidentiary support to the FormalAssertion.

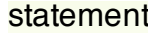
Superclass

EvidenceRelation

Semantics

Supports **relation is generated**  during evidence evaluation. It represents a relationship between an EvidenceItem and FormalAssertion objects where the EvidenceItem confers evidentiary support on the claim represented by FormalAssertion. This relationship is verbalized as: “EvidenceItem *supports* FormalAssertion.”

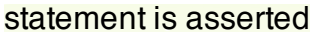
14.2.3 Challenges

Challenges **element**  represents an evidence relation between one EvidenceItem and one FormalAssertion element where the EvidenceItem challenges the validity of the FormalAssertion.

Superclass

EvidenceRelation

Semantics

Challenges **relation is generated**  during evidence evaluation. It represents a relationship between an EvidenceItem and FormalAssertion objects where the EvidenceItem is the so-called counter evidence to the claim represented by the FormalAssertion object, i.e., the EvidenceItem challenges the validity of the domain claim represented by the FormalAssertion. This relationship is verbalized as: “EvidenceItem *challenges* FormalAssertion.”

circumstantial evidence as it is often called) requires introduction of other pieces of information to complete a statement. Direct evidence has more weight than indirect. Whenever additional records are drawn to supply missing information there is a chance for error. Because of that, less weight is assigned to indirect evidence.

Support **characteristic** is verbalized as follows: **statement**

- “EvidenceItem directly supports FormalAssertion.”
- “EvidenceItem indirectly supports FormalAssertion.”
- “EvidenceItem directly challenges FormalAssertion.”
- “EvidenceItem indirectly challenges FormalAssertion.”

14.3.2 SupportLevel (enumeration)

SupportLevel enumeration specifies the support level.

Literals

- unknown
The directness is unknown.
- indirect
Evidence relation provides indirect support the Assertion.
- direct
Evidence relation provides direct support the Assertion.

14.3.3 Reporting

Reporting **element** **statement** represents a characteristic of the evidence relations that is asserted during the course of evaluation and that refers to the reporting level of the relationship - primary or secondary reporting - provided by evidence item to the corresponding claim.

Superclass

EvidenceAttribute

Attributes

- value:ReportingLevel
Reporting level of the evidence relation, such as secondary or primary.

Constaints

- Reporting element shall not be owned by elements other than EvidenceRelation.

Semantics

Reporting level is an asserted characteristic that potentially can be disputed. Reporting level ~~attribute adds a quality modifier to the EvidenceRelation. This characteristic~~ refers to the quality of information provided as evidence. For example, the record is primary if it was made at or near the time of the event, by someone in a position to know firsthand (such as an eyewitness). Alternatively, a record is considered primary if it was made in writing by an officer charged by law, canon, or bylaws with creating an accurate record. Primary information carries more weight than secondary

statement

information. Various communities disagree on whether primary information remains primary when copied. For example, the legal community states that a primary record becomes secondary when copied. Other communities focus on the information rather than the record, from which standpoint the primary information remains primary when copied.

Reporting **characteristic** is verbalized as follows: “EvidenceItem is a primary record of FormalAssertion,”
“EvidenceItem is a secondary record of FormalAssertion.”

14.3.4 ReportingLevel (enumeration)

ReportingLevel enumeration specifies the reporting levels.

Literals

- unknown
The level of reporting is unknown.
- secondary
EvidenceItem is a secondary record of FormalAssertion.
- primary
EvidenceItem is a primary record of FormalAssertion.

14.3.5 Accuracy

statement

Accuracy **element** represents characteristic of evidence relations that is asserted during the course of evaluation and that refers to the perceived accuracy of the information contained in the document. This characteristic refers to the level of trust the evaluator confers to the information contained in the document. Accuracy of the information affects the strength of evidentiary support this document provides. The Evidence Metamodel defines 5 levels of accuracy.

Superclass

DocumentAttribute

Attributes

- value: Level
Accuracy level of the Document, such as improbable, doubtful, possible, probable, confirmed.

14.3.6 AccuracyLevel (enumeration)

The AccuracyLevel enumeration class defines accuracy levels.

Literals

- unknown
Accuracy level is unknown.
- improbable
The information is improbable.
- doubtful
The information is doubtful.
- possible
The information is possible.

- probable
The information is probable.
- confirmed
The information is confirmed.

14.3.7 Confidence statement

Confidence **element** represents a characteristic of the evidence relations that is asserted during the course of evaluation and that refers to the confidence level of the relationship - whether information is reported as uncertain, plausible, or as a fact. Confidence affects the strength of evidentiary support provided by evidence item to the corresponding claim.

Superclass

EvidenceAttribute

Attributes

- value:ConfidenceLevel
Confidence level of the evidence relationship, such as reportedAsUncertain, reportedAsPlausible, reportedAsFact.

Semantics

Confidence **element is owned by EvidenceEvaluation as appropriate. Confidence characteristic is owned by EvidenceEvaluation object as appropriate. Each subclass of EvidenceEvaluation defines specific constraints regarding the meaning of Confidence in this context. Relevance** is an asserted characteristic that potentially can be disputed as opposed to EvidenceProperty, which represents fundamental properties of the EvidenceElement, and AdministrativeElement. Confidence ~~element includes the relevance~~ level.

14.3.8 ConfidenceLevel (enumeration) statement asserts the confidence

The ConfidenceLevel enumeration class defines confidence levels.

Literals

- unknown
Accuracy level is unknown.
- reportedAsUncertain
The information is reported as uncertain.
- reportedAsPlausible
The information is reported as plausible.
- reportedAsFact
The information is reported as Fact.

14.3.9 Significance statement

Significance **element** represents a characteristic of the evidence relations that is asserted during the course of evaluation and that refers to the significance level of the relationship - whether information that is reported as indirect support of the claim is significant to establish the truth of the claim. Significance affects the strength of evidentiary support provided by evidence item to the corresponding claim.

Superclass

EvidenceAttribute

Attributes

- value:Level
Significance level, such as low, mediumLow, medium, mediumHigh, or high.

14.3.10 Relevance statement

Relevance **element** represents a characteristic of the evidence relations that is asserted during the course of evaluation and that refers to the relevance level of the relationship - whether information that is reported as indirect support of the claim is relevant to establish the truth of the claim. Relevance affects the strength of evidentiary support provided by evidence item to the corresponding claim.

Superclass

EvidenceAttribute

Attributes

- value:Level
Relevance level, such as low, mediumLow, medium, mediumHigh, or high.

14.3.11 Level (enumeration)

Level enumeration provides generic 5-level qualitative measure. Level enumeration is utilized to evaluate relevance and significance of evidentiary support.

Literals

- unknown
The level is unknown.
- low
The level is low.
- mediumLow
The level is medium low.
- medium
The level is medium.
- mediumHigh
The level is medium high.
- high
The level is high.

14.3.12 Strength statement

Strength **element** represents characteristic of the evidence relations that is asserted during the course of evaluation and that refers to the reporting level of the relationship - the strength of the support relation - provided by evidence item to the corresponding claim.

Superclass

EvidenceAttribute

Attributes

- value:Integer
The strength of support: 0 to 100

Constraints

- Strength value shall be an integer value that is greater than or equal to 0 and less than or equal to 100.

Semantics

statement

Strength is an asserted characteristic that potentially can be disputed. Strength ~~attribute adds a quality modifier to the EvidenceRelation. This~~ characteristic refers to the quality of information provided as evidence. Strength can be a primary characteristic provided during the evaluation, or can be derived from other qualitative characteristics.

Strength ~~characteristic~~ is verbalized as follows: “EvidenceItem supports FormalAssertion with strength 50,”
“EvidenceItem challenges FormalAssertion with strength 10.”

14.3.13 ExtendedEvidenceAttribute

ExtendedEvidenceAttribute element represents a user-defined characteristic of the evidence relations that is asserted during the course of evaluation.

Superclass

EvidenceAttribute

Constraints

ExtendedEvidenceAttribute element shall own at least one TaggedValue describing the meaning of the element.

Semantics

ExtendedEvidenceAttribute is a user-defined characteristic. Its meaning is represented by the key-value pair of the corresponding TaggedValue element.

ExtendedEvidenceAttribute characteristic cannot be verbalized using the standard vocabulary of the Structured Assurance Case Metamodel. However, the key and value pair may be carefully named to result in meaningful verbalizations for the targeted community in the selected language.

14.4 EvidenceInterpretation Class Diagram

The EvidenceInterpretation Class Diagram defines several EvidenceEvaluation elements that allow assertions regarding the interpretation of EvidenceElements.

14.4.2 IsA

IsA statement represents a fundamental relation between one EvidenceElement and one FormalElement which defines the general concept for the subject EvidenceElement. The actual concept can be given by reference to an external formal vocabulary or ontology. The following statements are examples of IsA statements:

- “This metric is a McCabe’s Cyclomatic Complexity Metric.”
- “This report is a penetration testing report.”

Superclass

EvidenceInterpretation

Associations

- definition:FormalElement[1]
The formal FormalElement that is the general concept of the subject of the relation.

Constraints

- The subject of the IsA relation shall not be its definition.

Semantics

The IsA **statement** **element** asserts a state of affairs that the EvidenceElement, identified as the subject element of the IsScopedBy element, has a general concept represented by the FormalElement that is identified as the definition of the IsA element.

This **characteristic** is verbalized as follows: “EvidenceElement *is a* FormalElement.”

14.4.3 MeansThat

MeansThat **statement represents** **represents** a fundamental relation between one EvidenceElement and one FormalAssertion element which defines the meaning of the source EvidenceElement. The actual assertion is given by reference to an external formal vocabulary or ontology. The Evidence Metamodel limits the scope of meaning to a single fact type instance. Alternatively an informal ReferencedClaim can be used. The following statements are examples of Means:

- “This metric means that the quality of the system is medium-low.”
- “This report means that the preliminary hazard list has been identified correctly.”

Superclass

EvidenceInterpretation

Associations

- meaning:FormalAssertion[1]
FormalAssertion element

Constraints

- The subject of the MeansThat relation shall not be its meaning.

Semantics

statement

The MeansThat **element** asserts a state of affairs that the EvidenceElement, identified as the ‘subject’ of the MeansThat element, has meaning represented by the FormalAssertion that is identified as the ‘meaning’ of the MeansThat element.

This **characteristic** is verbalized as follows: “EvidenceElement *means that* FormalAssertion is true.”

14.4.4 IsCharacterizedBy

statement represents

IsCharacterizedBy **represents** a relation between one EvidenceElement and one FormalAssertion element that defines a characteristic of the subject EvidenceElement. The actual fact type is given by reference to an external formal vocabulary or ontology. The following statements are examples of IsCharacterizedBy:

- “This metric is characterized by its accuracy being confirmed,” or alternatively,
- “The accuracy of this metric is confirmed.”

Superclass

EvidenceInterpretation

Associations

- assertion:FormalAssertion[1]
The FormalAssertion that characterizes the subject EvidenceElement.

Semantics

statement

The IsCharacterizedBy **element** asserts a state of affairs that the EvidenceElement, identified as the ‘subject’ of the IsCharacterizedBy element, is characterized by an assertion, in which the subject is bound to one of the roles, and which is represented by the FormalAssertion that is identified as the ‘assertion’ of the IsCharacterizedBy element.

This **characteristic** is verbalized as follows: “EvidenceElement *is characterized by* FormalAssertion.”

14.4.5 IsScopedBy

IsScopedBy statement represents a relation between one EvidenceElement and one FormalElement that defines the scope of the subject EvidenceElement. The actual concept is given by reference to an external formal vocabulary or an ontology. The following statements are example of IsScopedBy: “This metric is scoped by the client subsystem.”

Superclass

EvidenceInterpretation

Associations

- scope:FormalElement[1]
The FormalElement that is the scope of the subject of the relation.

Constraints

- The subject of the IsScopedBy relation shall not be its scope.

Semantics

statement

“Scope” is defined as the area covered by a given activity or subject, which can be interpreted in either physical or logical sense. The IsScopedBy **element** asserts a state of affairs that the EvidenceElement, identified as the ‘subject’ of the IsScopedBy element, is delimited by the FormalElement that is identified as the ‘scope’ of the IsScopedBy element. The FormalElement may represent an individual concept, an abstract concept or an assertion.

This **characteristic** is verbalized as follows: “EvidenceElement *is scoped by* FormalElement.”

14.4.6 ProvidesContext

ProvidesContext **element represents statements that assert** that a certain evidence element provides a context for the interpretation of another evidence element.

statement asserts

Superclass

EvidenceInterpretation

Associations

- context:EvidenceElement[1]
The element that is asserted to represent the context for the subject.

Semantics

statement

ProvidesContext **element** establishes a relationship between two evidence elements where the ‘context’ evidence element (usually an EvidenceGroup) provides a context for the ‘subject’ evidence element (usually a FormalAssertion, or an EvidenceAssertion). A ‘context’ is defined as the set of evidence elements (including evidence items, evidence assertions, and even project elements) that are important for understanding of the ‘subject’ evidence element. The concept of a context is more informal than the related concept of ‘scope’ (see ‘IsScopedBy’ assertion).

14.5 Evidence Observations Class Diagram

The EvidenceObservations Class Diagram defines several EvidenceEvaluation elements that allow assertions regarding the dependencies between EvidenceRelation elements or conflicts between FormalAssertions.

Abstract class EvidenceEvaluation has been introduced earlier in section 10.2 EvidenceAssertions during the overview of the Evidence Metamodel. Instances of EvidenceObservation are owned directly by EvidenceContainer (see section 15 Administration)

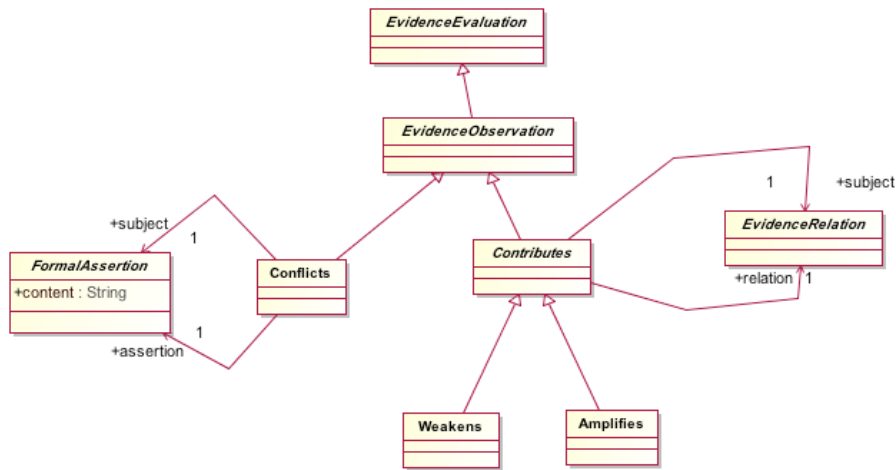


Figure 14.4 - EvidenceObservations Class Diagram

14.5.1 EvidenceObservation (abstract)

represents various statements that assert

EvidenceObservation is an abstract class that asserts existence of a dependency between two evidence relations or conflict between two domain assertions. These conflicts need to be further addressed during the rest of the evidence evaluation process.

Superclass

EvidenceEvaluation

Semantics

statement

The EvidenceObservation element asserts existence of a conflict in evidentiary support. The concrete subclasses of the EvidenceObservation element define the exact nature of the conflict.

14.5.2 Conflicts

Conflicts element asserts existence of a conflict between two domain assertions. For example, one may assert that the claim that “Bob is married to Alice” conflicts the claim that “Bob is single” and conflicts the claim that “Bob is married to Eve.” These conflicts need to be further addressed during the rest of the evidence evaluation process.

Superclass

EvidenceObservation

Associations

- subject: FormalAssertion[1]
The subject FormalAssertion
- assertion: FormalAssertion[1]
The object FormalAssertion

Semantics

The Conflicts **element** asserts a state of affairs that the FormalAssertion-1, identified as the assertion1 of the Conflicts element, is in conflict with FormalAssertion that is identified as the assertion2 of the Conflicts element. Conflict here is defined as a state of doubt that both assertions can be true at the same time. The conflict needs to be resolved by clarifying the meaning of the assertions, negating or refuting the supporting evidence to one of the assertions, etc.

This **characteristic** is verbalized as follows: "FormalAssertion-1 *conflicts* FormalAssertion-2"

14.5.3 Contributes (abstract)

Contributes **element** asserts dependency between two EvidenceRelation elements. For example, let's assume the following evidentiary relationships:

Exhibit A *supports* (referenced) claim that "Bob *is married to* Alice"

Exhibit A *challenges* claim "Bob *is single*"

We can observe that **the claim** "Bob *is married to* Alice" *conflicts with* **the claim** "Bob *is single*"

Let's further assume the following evidentiary relationship:

Exhibit C *supports* claim Exhibit A is likely a forgery

We can observe that:

The evidence assertion Exhibit C supports claim "Exhibit A is likely a forgery" *weakens support* given by **the** Exhibit A to the claim "Bob *is married to* Alice"

At the same time we do not directly assert that:

Exhibit C *challenges* **the claim** "Bob *is married to* Alice"

Evidence observations help capture dependencies between related claims and thus facilitate evaluation of evidence.

Superclass

EvidenceObservation

Associations

- subject: EvidenceRelation[1]
The subject EvidenceRelation
- relation: EvidenceRelation[1]
The object EvidenceRelation

Constraints

The subject and object EvidenceRelation elements shall not be the same.

Semantics

The Contributes **element** asserts existence of a dependency in evidentiary support. The concrete subclasses of the Contributes element define the exact nature of the dependency.

14.5.4 Weakens

Weakens **element** asserts that the subject EvidenceRelation weakens another EvidenceRelation2. This statement has a different meaning than a statement about existence of an evidence item that (directly) challenges the FormalAssertion involved in the EvidenceRelation2. Weakens relation may imply a conflict between the subject FormalAssertion that is involved in the subject EvidenceRelation and FormalAssertion2. In that case the evidence in support of the subject FormalAssertion is not relevant to FormalAssertion2.

Superclass

Contributes

Semantics

The Weakens **element** asserts a state of affairs that the EvidenceRelation-1, identified as the 'subject' of the Weakens element, weakens EvidenceRelation-2 that is identified as the 'relation' of the Weakness element. The Weakens statement asserts a negative contribution made by one EvidenceEvaluation to another EvidenceEvaluation. Weakens may imply a conflict between the 'subject' FormalAssertion-1 that is identified as assertion of EvidenceRelation-1 and FormalAssertion-2 that is identified as assertion of EvidenceRelation-2.

This **characteristic** is verbalized as follows: "Evidentiary support to FormalAssertion-1 weakens evidentiary support to FormalAssertion-2", where the statement "Evidentiary support to a FormalAssertion C1" is an objectified assertion that there is an evidence item E1 that supports the FormalAssertion C1".

14.5.5 Amplifies

Amplifies **element** asserts that the subject EvidenceRelation amplifies another EvidenceRelation2. This statement has a different meaning than the statement asserting existence of an evidence item that (directly) supports the FormalAssertion2 that is involved in the EvidenceRelation2. Amplifies relation may imply a coupling between the subject FormalAssertion and the FormalAssertion2. In that case the evidence in support of the subject FormalAssertion may be relevant to the FormalAssertion.

Superclass

Contributes

Semantics

The Amplifies **element** asserts a state of affairs that the EvidenceRelation-1, identified as the subject, amplifies EvidenceRelation-2 that is identified as the relation of the Amplifies element. The Amplifies statement asserts a positive contribution made by one EvidenceEvaluation to another EvidenceEvaluation. Amplifies may imply a coupling between FormalAssertion-1 that is identified as assertion of EvidenceRelation-1 and FormalAssertion-2 that is identified as assertion of EvidenceRelation-2.

This **characteristic** is verbalized as follows: "Evidentiary support to the subject FormalAssertion amplifies evidentiary support to FormalAssertion2".

14.6 Evidence Resolutions Class Diagram

The EvidenceResolutions Class Diagram defines several EvidenceEvaluation elements that allow assertions regarding the resolutions to EvidenceEvaluation elements for the purpose of explaining the conflicts between FormalAssertions. The Evidence Metamodel provides three options: Negate EvidenceRelation, Refute a FormalAssertion, and Resolve

EvidenceObservation (which implies existence of conflicting claims). The purpose of EvidenceResolutions is to provide necessary clarifications explaining the existence of counterevidence to the key domain claims. At the end of evidence evaluation EvidenceResolutions should build a clear picture showing that the preponderance of evidence to the required domain claims in case of real conflicts, and resolving the conflicts that are determined by imprecise formulation of claims and incorrect interpretation of evidence.

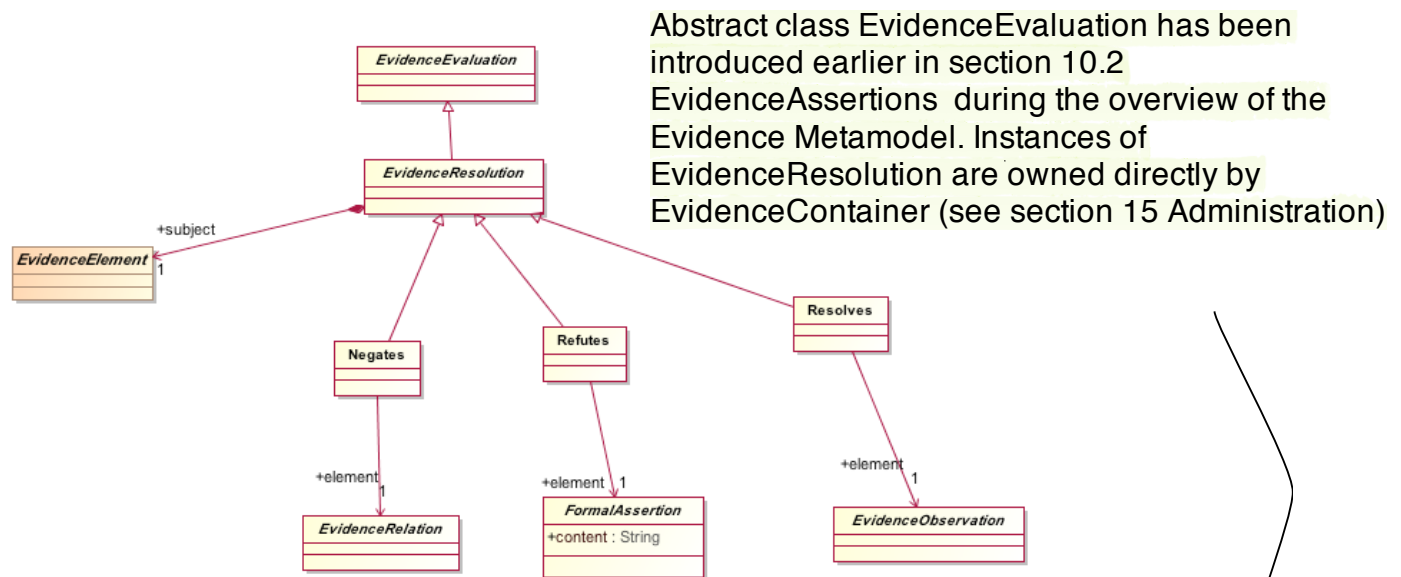


Figure 14.5 - EvidenceResolutions Class Diagram

14.6.1 EvidenceResolution (abstract)

EvidenceResolution represents statements that assert resolution to the conflicts between two evidence assertions either directly or indirectly by refuting some evidence assertion or negating some evidence relation.

Superclass

EvidenceEvaluation

Associations

- subject: EvidenceElement[1]
The subject evidence element for the resolution, i.e., the evidence element negates, resolves, or refutes other evidence elements.

Constraints

- The EvidenceElement that is resolved by the EvidenceResolution (as defined by one of the concrete subclasses of the EvidenceResolution class) shall not be a member of the context either directly or indirectly through membership in other contexts.

Semantics

statement

The EvidenceResolution element asserts resolution of a conflict in evidentiary support. The concrete subclasses of the EvidenceResolution element define the exact nature of the resolution.

14.6.2 Negates

Negates **element** asserts negation of an EvidenceRelation. For example, one may want to assert that “there is insufficient evidence to support the fact that the weakness in line 256 can be exploited by an outside attacker.” Negation indirectly refutes the FormalAssertion by claiming that the evidentiary support to the FormalAssertion is indirect, weak, unreliable, not coming from credible sources.

Superclass

EvidenceEvaluation

Associations

- element:EvidenceRelation[1]
The EvidenceRelation being negated.

Semantics

The Negates **element** asserts negation of evidentiary support to a certain FormalAssertion. The Rationale element that is owned by the Negates object provides a readable explanation to the negation. The context property may refer to a particular set of EvidenceAttribute or Document that describes the context for negation. Negates **element** addresses the existing evidentiary support to a certain FormalAssertion.

14.6.3 Refutes

Refutes **element** asserts direct refutation of a FormalAssertion. For example, one may want to assert that “the weakness in line 256 cannot be exploited by an outside attacker because of the existence of proper architecture controls.” Refutes **element** asserts direct refutation of a FormalAssertion. Context of the refutation is important, because the conflicting claims with strong evidentiary support need to be identified.

Superclass

EvidenceEvaluation

Associations

- element:FormalAssertion[1]
The FormalAssertion being refuted.

Semantics

The Refutes **element** asserts direct refutation of a certain FormalAssertion. The Rationale element that is owned by the Refutes object provides a readable explanation to the refutation. The context property may refer to a particular set of EvidenceAttribute or Document that describe the context for refutation. Refutes **element** emphasizes the claims with strong evidentiary support conflicting to the FormalAssertion being refuted.

14.6.4 Resolves

Resolves **element** asserts resolution of a conflict between two FormalAssertions. For example, one may want to assert that “the fact that Bob is married to Alice is not in conflict with the fact that Bob is single because they refer to non-overlapping time intervals.” Resolves **element** asserts resolution to a conflict between two FormalAssertions. Context of the resolution is important, because the precise interpretation of the seemingly conflicting claims with strong evidentiary support need to be identified.

statement

Superclass

EvidenceEvaluation

statement

Associations

- element:EvidenceObservation[1]
The EvidenceObservation being resolved (usually a Conflicts relation between two FormalAssertions).

Semantics

The Resolves **element** asserts resolution of a conflict between two FormalAssertions. The Rationale element that is owned by the Resolves object provides a readable explanation to the resolution. The context property may refer to a particular set of EvidenceAttribute or EvidenceInterpretation that describe the context for resolution. Resolves **element** emphasizes the claims with strong evidentiary support are not conflicting after precise interpretation.

15 Administration

15.1 General

evidence assertions

This clause describes the elements of the SACM Evidence Metamodel that are involved in managing evidence, exchanging units of evidence, and related concerns. The elements described in this clause organize instances on Evidence Metamodel, which can be referred to as an Evidence Model. In particular, this clause defines the root object of Evidence Models - the EvidenceContainer. This element contains other objects in an evidence project and constitutes a unit of exchange using the Evidence Metamodel as the protocol.

15.2 Project Class Diagram

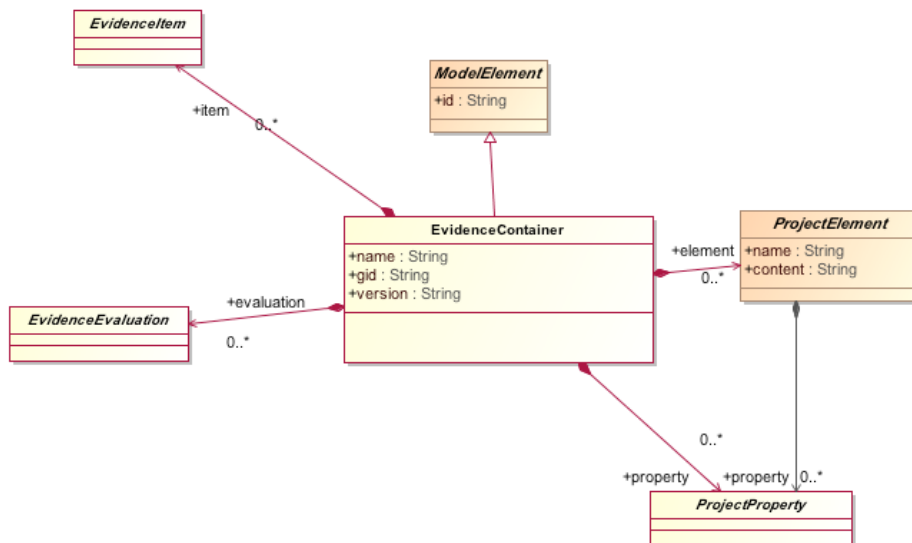


Figure 15.1 - Project Class Diagram

15.2.1 ProjectElement (abstract)

ProjectElement represents the auxiliary elements of the Evidence Metamodel that are involved in the statements related to managing evidence collection, interpretation, evaluation, and exchange processes.

Superclass

EvidenceElement

Attributes

- name:String
Name of the ProjectElement.
- content:String
Statement in a selected language that is the description of the content of the element.

Associations

- `property:ProjectProperty[0..*]`
Properties of the ProjectElement - zero or more predicates to the main clause in which the current element is the subject.

Semantics

statements associated with

The **properties of** a ProjectElement make assertions regarding the current element (use the current element as the subject of the corresponding clauses). Therefore, the following **properties for** a ProjectElement can be readily interpreted in the above way:

elements owned by

- *DependsOn* when a subject element is an Activity (for example, verbalized as “Activity A2 depends on Activity A1”).
- *HasRoleIn* when the subject element is a Stakeholder (for example, verbalized as “Bob is president of organization SupplierCorporation”).
- *Satisfies* when a subject element is an Activity (for example, verbalized as “Activity A2 satisfies project objective Perform Search”).

All ProjectProperties clauses directly owned by a ProjectElement shall be interpreted with the ProjectElement as the main subject. For example, “Person Researcher depends on activity Perform Search and satisfies project objective Find evidence.”

15.2.2 EvidenceContainer

EvidenceContainer element is the root object of the SACM Evidence Metamodel instances. This object owns EvidenceItem, and EvidenceEvaluation elements, as well as other ProjectElement related to the processes of evidence identification, collection, interpretation, evaluation, and management.

Superclass

EvidenceElement

Attributes

- `name:`
String name of the EvidenceContainer.
- `gid:`
String Globally unique identifier of the EvidenceContainer.
- `version:`
String version of the EvidenceContainer.

Association

- `item:EvidenceItem[0..*]`
List of evidence items.
- `evaluation:EvidenceEvaluation[0..*]`
List of evaluations.
- `element:ProjectElement[0..*]`
List project elements (objectives, activities, requests, methods, stakeholders).

- `property:ProjectProperty[0..*]`
List of project property clauses.

Constraints

- EvidenceContainer shall not be the object of the requiresContainer relation owned by the EvidenceContainer, either directly or indirectly through requiresContainer of other EvidenceContainers.
- Any EvidenceContainer that is the object of the requiresContainer relation shall be available for exchange.
- [Completeness of the evidence container with respect to required evidence containers]
Any Element that is referenced by any of the Elements defined in the package (i.e., that are members of the lists item, evaluation, or element of the EvidenceContainer) shall be defined also in the EvidenceContainer or in one of the EvidenceContainers that are referred to as objects of the requiresContainer relation either directly or indirectly. An Element is referenced if it is an object of an EvidenceProperty or an EvidenceEvaluation.
- EvidenceProperty, EvidenceEvaluation, EvidenceRequest, EvidenceAction, ProjectObjective elements shall not be referenced across evidence containers.

Semantics

statements associated with

EvidencePackage element is the root object of an instance of the Evidence Metamodel (which can be referred to as Evidence Model). A single EvidenceContainer is a unit of exchange of evidence information. All Elements defined in an EvidenceContainer are exchanged together as part of the EvidenceContainer. Elements that are referenced shall be either present in the EvidenceContainer or in one of the EvidenceContainers that is specified as required for the EvidenceContainer. The Evidence Metamodel does not require completeness of the closure of all required packages.

The **properties of** the EvidenceContainer element make assertions regarding the current container (use the current container as the subject of the corresponding clauses). Therefore, the following **properties for** an EvidenceContainer can be readily interpreted in the above way:

elements owned by

- RequiresContainer (for example, verbalized as “the EvidenceContainer *requires* EvidenceContainer X1”).
- ContainerConsistency (for example, verbalized as “elements of the EvidenceContainer *are interpreted formally*”).
- ContainerCompleteness (for example, verbalized as “the EvidenceContainer *is in draft state*”).
- CompliesTo (for example, verbalized as “the EvidenceContainer *complies to* Resolved Counter Evidence proof standard”).

All ProjectProperties clauses directly owned by an EvidenceContainer shall be interpreted with the EvidenceContainer as the main subject. For example, “the EvidenceContainer *depends on* evidentiary support rendered by Exhibit E1 to Claim Testing is completed.”

15.3 ProjectElements Class Diagram

ProjectElements Class Diagram defines several auxiliary elements that are used in various statements as predicate clauses for some main clause **in which the subject** is some evidence element. The elements defined at this class diagram are collectively referred to as the project elements. They are required to express various evidence statements related to evidence collection, evaluation, and evidence management.

Semantics

statement asserts

RequiresTool ~~is an owned property of Service. This property represents~~ a state of affairs that the tool identified as tool attribute of the RequiresTool object owned by Service object, is required by the Service object. Further detail may be provided through the Provenance and Timing ~~attribute~~. Multiple OwnedBy attribute specifies multiple providers of the Service.

clauses

15.3.5 Method

Method element represents an evidence collection method that can be applied by a person or an organization. The scope of a Method may be creation, acquisition, and generation of evidence elements, transfer of evidence element, revocation of evidence elements, evaluation of evidence elements.

Superclass

CollectionMethod

Associations

- tool:RequiresTool[0..*]
Tool that is required by the method.

Semantics

statement asserts

RequiresTool ~~is an owned property of Method. This property represents~~ a state of affairs that the tool identified as tool attribute of the RequiresTool object owned by Method object, is required by the Method object. Further detail may be provided through the Provenance and Timing ~~attribute~~. Multiple OwnedBy attribute specifies multiple providers of the Method.

clauses

15.3.6 Tool

Tool element represents an automated evidence collection or evidence generation capability that can be licensed by a person or an organization.

Superclass

CollectionMethod

Attributes

- version:String[1]
Designation of the version of the tool.

15.3.7 Stakeholder (abstract)

Stakeholder is an abstract class that represents a Person or an Organization as they participate in the statements related to evidence.

Superclass

ProjectElement

Semantics

The Evidence Metamodel indirectly defines several roles in which stakeholders are involved in evidence statements, such as Provenance statements and Custody statements. These roles include the “source” of an evidence item or an evidence assertion, the “supervisor” of an evidence assertion, the “owner” of an evidence item, the ‘executor’ of an evidence event and the “custodian” of an evidence item. This vocabulary facilitates exchange of structured statements related to evidence. Additional roles related to the affiliation of a stakeholder in some Organization can be defined by the corresponding community of interest. These roles can be used in HasRoleIn statements and exchanged informally, as the value of the ‘role’ attribute. On the other hand, formal statements related to stakeholders and their roles can be represented using the mechanism of Formal Statements. The fact type “stakeholder *has role with respect to* evidence item” can be formally defined outside of the Evidence Metamodel and then referred to for the purpose of constructing formal statements related to stakeholders.

15.3.8 Person

An individual that can be the source of evidence items in various roles defined by the Evidence Metamodel. A person may be affiliated with an Organization.

Superclass

Stakeholder

Associations

- affiliation:HasRoleIn[0..1]
Affiliation of the Person with an Organization.

Semantics

statement asserts

HasRoleIn ~~is an owned property of Person. This property represents~~ a state of affairs that the Person identified as organization attribute of the HasRoleIn object owned by Person object, is the organization with which the Person is affiliated in the role identified as the ‘role’ attribute of the HasRoleIn object. Further detail may be provided through the Provenance and Timing ~~attribute~~. For example, EffectiveTime ~~property~~ is added specifies the effective period of affiliation. Person may be affiliated with multiple organizations.

clause

15.3.9 Organization

clauses

An organization that can be the source of evidence items in various roles defined by the Evidence Metamodel. Organization may be affiliated with another Organization.

Superclass

Stakeholder

Attributes

- address:String
The address of the Organization.

Associations

- affiliation:HasRoleIn[0..1]
Affiliation of the Organization with parent Organization.

Constraints

Organization shall not be affiliated with self, either directly or indirectly.

Semantics

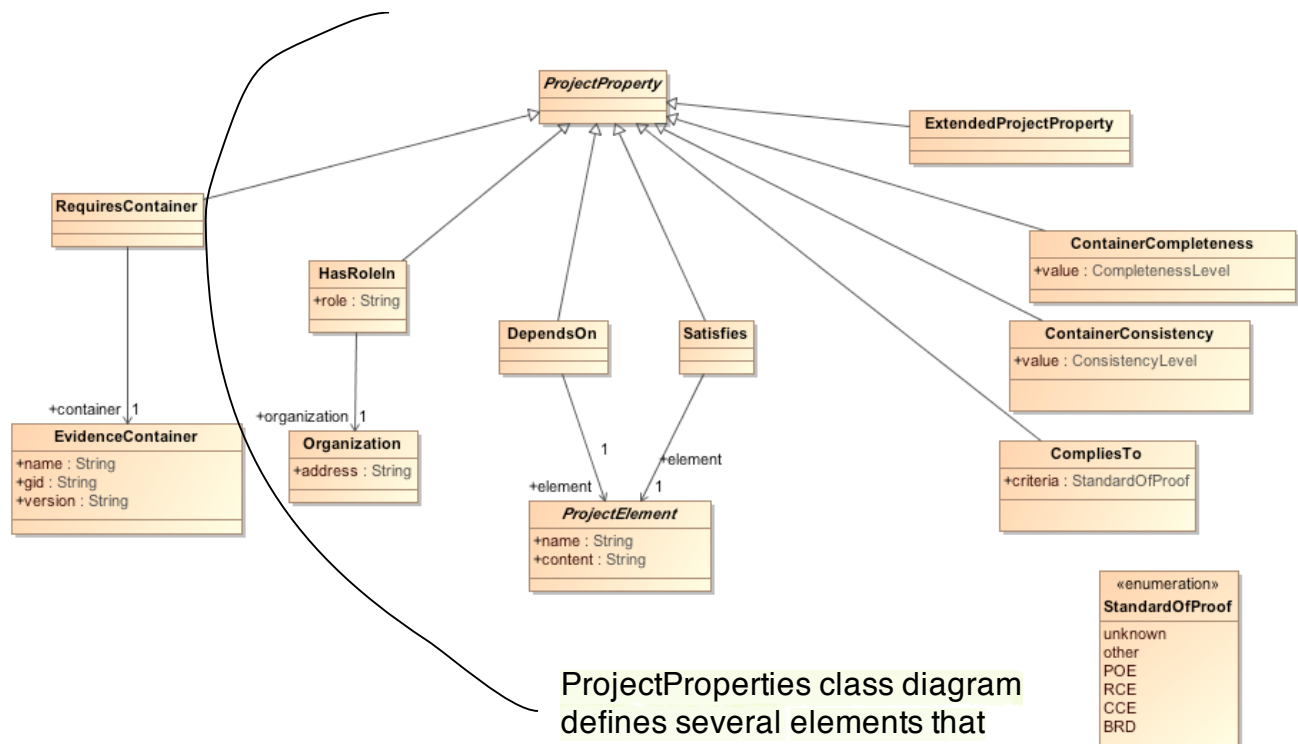
statement asserts

HasRoleIn is an owned property of Organization. This property represents a state of affairs that the Organization-2 identified as organization attribute of the HasRoleIn object owned by Organization-1 object, is the organization with which the Organization-1 is affiliated in the role identified as the 'role' attribute of the HasRoleIn object. Further detail may be provided through the Provenance and Timing attribute. For example, EffectiveTime property is added specifies the effective period of affiliation. Organization may be affiliated with multiple other organizations.

15.4 ProjectProperties Class Diagram

clauses

clause



ProjectProperties class diagram defines several elements that represent various statements related to project elements.

Figure 15.3 - ProjectProperties class diagram

15.4.1 ProjectProperty (abstract)

ProjectProperty represents statements related to the structure of ProjectElement. These statements are predicate clauses where the main clause describes some project element. The subject of the ProjectProperty clause is a ProjectElement.

Superclass

EvidenceProperty

Semantics

Defined by concrete subclasses

15.4.2 Satisfies

statement asserts

statement

Satisfies **element represents** a relationship between the owner project element and another project element that is identified as the element attribute of the Satisfies element. The Satisfies **element** is a clause where the main subject is the ProjectElement that owns the current element. For example, this clause can be used to specify that a certain Activity satisfies a certain ProjectObjective in an evidence-related effort.

Superclass

ProjectProperty

Associations

- element:ProjectElement[1]
Project element (such as a ProjectObjective) that is satisfied by the subject project element.

Semantics

statement asserts

Satisfies **element represents** a state of affairs that the subject project element object satisfies another ProjectElement (such as a ProjectObjective) identified as the 'element' attribute of the Satisfies element.

15.4.3 HasRoleIn

~~An owned property~~ of Person and Organization.

Superclass

ProjectProperty

HasRoleIn statement asserts an affiliation

Attributes

- role:String
The role in which Person or Organization is affiliated with another Organization.

Associations

- organization:Organization[1]
Organization with which the subject ProjectElement (such as Person or Organization) is affiliated in the given role.

Constraints

- ProjectElement shall not be affiliated with self, either directly or indirectly.

15.4.4 DependsOn

statement asserts

statement

DependsOn **element represents** a relationship between the owner project element and another project element that is identified as the element attribute of the DependsOn element. DependsOn **element** is a clause where the main subject is the ProjectElement that owns the current element. For example, this clause can be used to specify dependencies between Activities in an evidence-related effort.

Superclass

ProjectProperty

Associations

- element:ProjectElement[1]
Project element that the subject element depends on.

Constraints

- ProjectElement shall not depend on self, either directly or indirectly.

Semantics

statement asserts

DependsOn ~~element represents~~ a state of affairs that the subject project element depends on another project element identified as the 'element' attribute of the DependsOn element.

Dependency of one ProjectElement on another can have various meanings. The SACM Evidence Metamodel does not provide a normative enumeration of the nature of dependency. However, should an author of a SACM document desire so, a TaggedValue mechanism shall be used for this purpose with a tag 'natureofdependency.'

15.4.5 StandardOfProof (enumeration)

The StandardOfProof enumeration defines the values of the standard of proof criteria for evidence evaluation.

Literals

- unknown
Standard of Proof unknown
- other
Standard of proof other than those explicitly enumerated
- POE
Preponderance of Evidence
- RCE
Resolved Counter Evidence
- CCE
Clear and Convincing Evidence
- BRD
Beyond Reasonable Doubt

Semantics

There are well-defined "Standards of proof," such as:

- Preponderance of evidence (POE), also known as the balance of the probabilities. The standard is met if the proposition is more likely to be true than not true. This standard is required in most civil cases.
- Resolved Counter Evidence (RCE) - this standard is met if all the evidence points in the same direction and anything to the contrary must be resolved. This is a stricter standard than the preponderance of evidence, where even a slight tipping of the scale is sufficient.
- Clean and Convincing Evidence (CCE) - this standard is met if it is substantially more likely than not that the proposition is in fact true. This is a lesser requirement than "proof beyond a reasonable doubt," which requires that the proposition be close to certain of the truth, but a stricter requirement than proof by "preponderance of the evidence," which merely requires that the proposition asserted seem more likely true than not.

- Beyond the reasonable doubt (BRD) this standard is met if the proposition being presented is proven to the extent that there is no “reasonable doubt” in the mind of a reasonable person that the proposition is true. There can still be a doubt, but only to the extent that it would not affect a “reasonable person’s” belief that the proposition is true.

15.4.6 RequiresContainer

statement asserts

RequiresContainer ~~is an owned property of EvidenceContainer element. This element represents a statement asserting~~ that the subject EvidenceContainer requires another evidence container for the resolution of some references.

Superclass

ProjectProperty

Associations

- container:EvidenceContainer[1]
EvidenceContainer that is required for the resolution of some references in the subject evidence container.

Constraints

- RequiresContainer element shall not be owned by any ProjectElement object.
- subject EvidenceContainer shall not be the ‘container’ of the requiresContainer relation, either directly or indirectly.

Semantics

statement asserts

statement

RequiresContainer ~~property represents~~ a state of affairs that the subject EvidenceContainer requires another evidence container for the resolution of some references. This ~~property~~ contributes to the completeness constraint of the EvidenceContainer. This is a commitment to the set of evidence containers that need to be processed together.

15.4.7 ContainerConsistency

statement

statement related to

ContainerConsistency ~~element~~ is a counterpart of the Consistency ~~property of~~ Documents. ContainerConsistency clause makes an assertion about the subject EvidenceContainer regarding the level of formality of the element of the container. In combination with other container properties, such as ContainerCompleteness and CompliesTo, this clause determines capability to interpret the elements of this container. Consistency of an EvidenceContainer can be informal, semiformal, and formal.

Superclass

ProjectProperty

Attributes

- value:ConsistencyLevel
asserted Consistency level of the elements of the EvidenceContainer, such as informal, semi-formal, and formal.

15.4.8 ContainerCompleteness

statement

statement related to

ContainerCompleteness **element** is a counterpart of the Completeness **property of** Documents. ContainerCompleteness clause makes an assertion about the subject EvidenceContainer regarding the level of completeness of the element of the container. In combination with other container properties, such as ContainerConsistency and CompliesTo, this clause determines capability to interpret the elements of this container. Completeness of an EvidenceContainer can be incomplete, draft, final, and obsolete.

Superclass

ProjectProperty

Attributes

- value:CompletenessLevel
asserted Completeness level of the elements of the EvidenceContainer, such as incomplete, draft, final, and obsolete.

15.4.9 CompliesTo

CompliesTo clause makes an assertion about the subject EvidenceContainer regarding the standard of proof used for the evaluation of evidence in the EvidenceContainer. In combination with other container properties, such as ContainerConsistency and ContainerCompleteness, this clause determines capability to interpret the elements of this container. Completeness of an EvidenceContainer can be incomplete, draft, final, and obsolete.

Attributes

- criteria:StandardOfProof
Standard of Proof used for evaluation of evidence in the subject container.

15.4.10 ExtendedProjectProperty

ExtendedProjectProperty element represents a user-defined characteristic documents that is asserted during the course of evaluation for the project elements in the subject container.

Superclass

ProjectProperty

Constraints

ExtendedProjectProperty element shall own at least one TaggedValue informally describing the meaning of the element.

Semantics

ExtendedProjectProperty is a user-defined characteristic. Its meaning is represented by the key-value pair of the corresponding TaggedValue element.

ExtendedProjectProperty characteristic cannot be verbalized using the standard vocabulary of the Structured Assurance Case Metamodel. However, the key and value pair may be carefully named to result in meaningful verbalizations for the targeted community in the selected language.