

8 SACM Assurance Case

8.1 Administration Class Diagram

This sub clause describes the common elements of SACM that are involved in managing assurance cases, exchanging assurance cases, and related concerns. The elements described in this clause organize instances of SACM. In particular, this sub clause defines the root object of an assurance case - the AssuranceCase element. This element contains other objects in an assurance case, such as the Argumentation objects and EvidenceContainer objects and constitutes a unit of exchange using the SACM as the protocol.

In addition, the SACM Argumentation Metamodel and the SACM Evidence Metamodel constitute two independent protocols within SACM, so Argumentation packages can be developed and exchanged using the Argumentation elements, and the EvidenceContainers can be developed, managed, and exchanged independently of the Argumentation elements or in combination with them. Independently developed Argumentation packages and EvidenceContainer packages can be later assembled into complete assurance cases. Specifications of the Evidence Metamodel can be used to develop an evidence repository that can be used to store and manage evidence in support of multiple assurance cases.

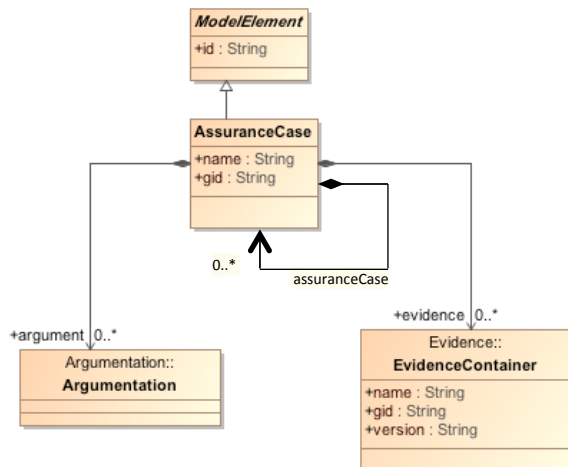


Figure 8.1 - Administration Class Diagram

8.1.1 AssuranceCase

AssuranceCase element

Superclass

ModelElement

Attributes

- name:String
the name of an assurance case

- assuranceCase:AssuranceCase[0..*]
the nested AssuranceCase contained in a given instance of an AssuranceCase.

- gid:String
the globally unique identifier assigned to the current assurance case

Associations

- Argumentation::Argumentation[0..*]
the argument component of an assurance case
- Evidence::EvidenceContainer[0..*]
the evidence component of an assurance case

Semantics

An AssuranceCase element represents assurance cases as defined in ISO/IEC 15206. Argument and Evidence components of an AssuranceCase are optional, which allows representing incomplete assurance cases.

An AssuranceCase element involves both a globally unique “gid” and a locally unique “id.” The global referencing scheme may involve gid+id combination, while a local scheme may use id component.

AssuranceCase shall have a globally unique gid attribute.

Constraints

gid is a string that has the following structure:

- unique url of the organization that created an assurance case
- the text ‘AssuranceCase’
- a unique number

For each contained object of an assurance case the gid+id identifier is globally unique, i.e., no two elements of the same type produced by the same organization shall have the same number.

8.2 CommonElements Class Diagram