# Software Assurance Evidence Metamodel final submission

Nikolai Mansourov
KDM Analytics

Presented March, 22 2010, OMG Technical Meeting, Jacksonville, FL

# Status

- ***Submitted by:***
  - ***KDM Analytics***
  - ***Lockheed Martin,***
  - ***Computer Sciences Corporation,***
  - ***Benchmark Consulting,***
  - ***NIST***
  - ***Adelard LLP***
  - ***University of York***
- ***Supported by:***
  - ***MITRE,***
  - ***SEI***

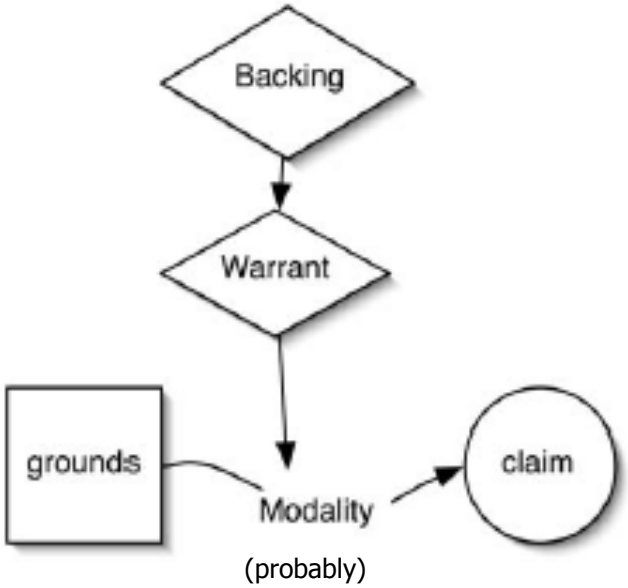
Initial submission: Feb 2008
Revised submission: Aug 2008
2nd Revised submission: Aug 2009
Final submission: March 2010

# What is Assurance Case ?

- Assurance Case
  - Set of auditable claims, arguments and evidence created to support the claim that a defined system/service will satisfy the particular requirements
  - It enables suppliers and acquirers to represent their claims and arguments (respectively), along with the corresponding evidence

- Key concepts
  - Systems Assurance makes claims
    - Claims are structured to facilitate communication
  - Certain claims are supported through reasoning
    - Reasoning is expressed by annotated links between claims
  - Certain claims are supported through evidence
    - Evidence is collected by applying systematic methods and procedures
    - In the software assurance context, evidence is often collected by tools
  - Certain associations between claims and subclaims are justified
    - Justification explains the selection of argument strategy
  - Claims are propositions
    - Propositions are expressed by statements

# Support by 'Substantial' Reasoning

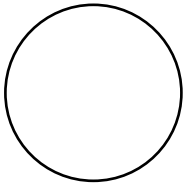



- Claims are assertions put forward for general acceptance
- The justification for claim is based on some grounds, the "specific facts about a precise situation that clarify and make good for a claim"
- The basis of the reasoning from the grounds (the facts) to the claim is articulated. Toulmin coined the term "warrant" for "substantial argument". These are statements indicating the general ways of argument being applied in a particular case and implicitly relied on and whose trustworthiness is well established".
- The basis of the warrant might be questioned, so "backing" for the warrant may be introduced. Backing might be the validation of the scientific and engineering laws used

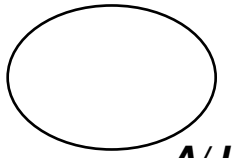
# The Goal Structuring Notation (GSN)

## Purpose of a Goal Structure

To show how goals  are broken down into sub-goals,

and eventually supported by evidence (solutions) 

whilst making clear the strategies  adopted,

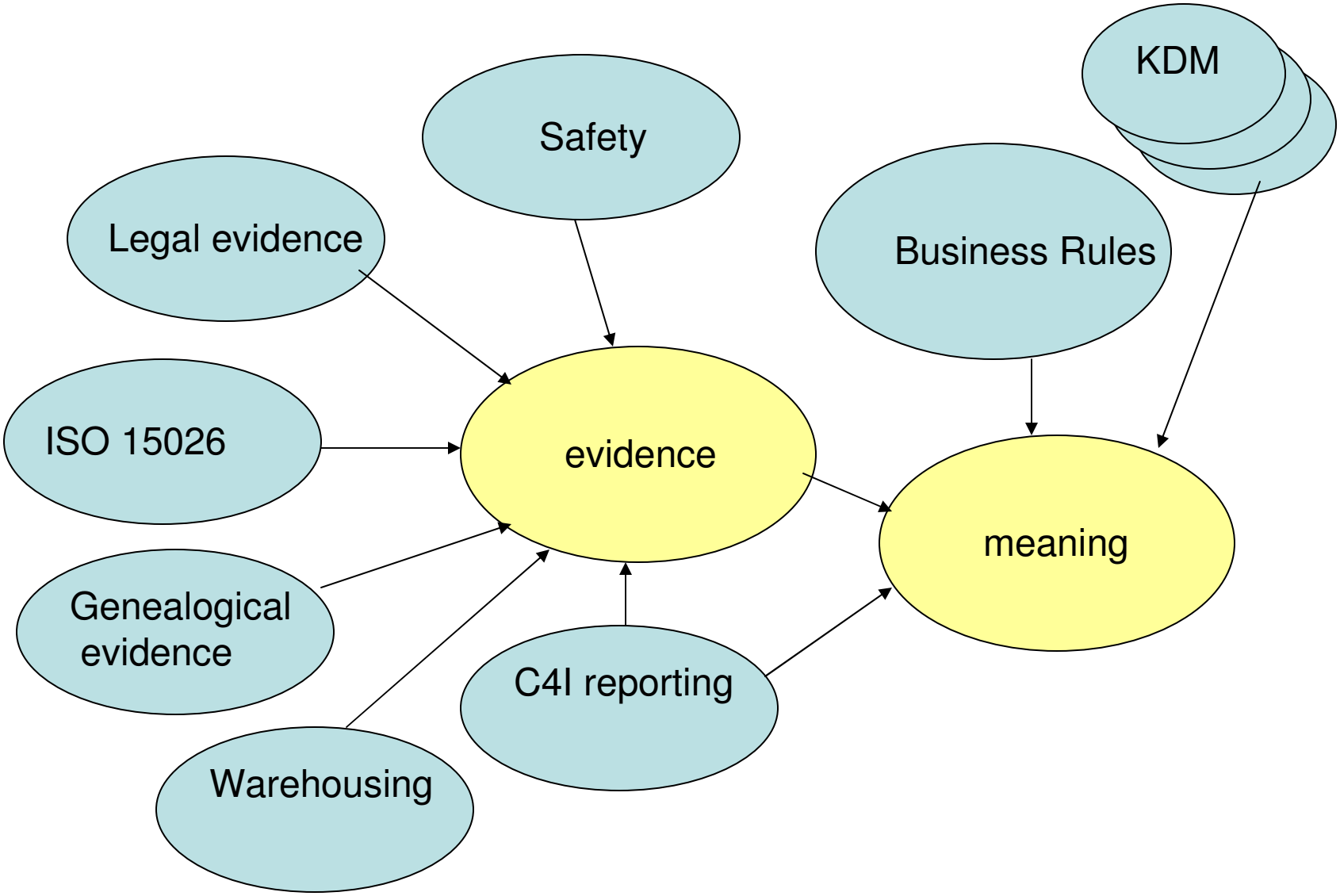
the rationale for the approach (assumptions, justifications) 


and the context  in which goals are stated

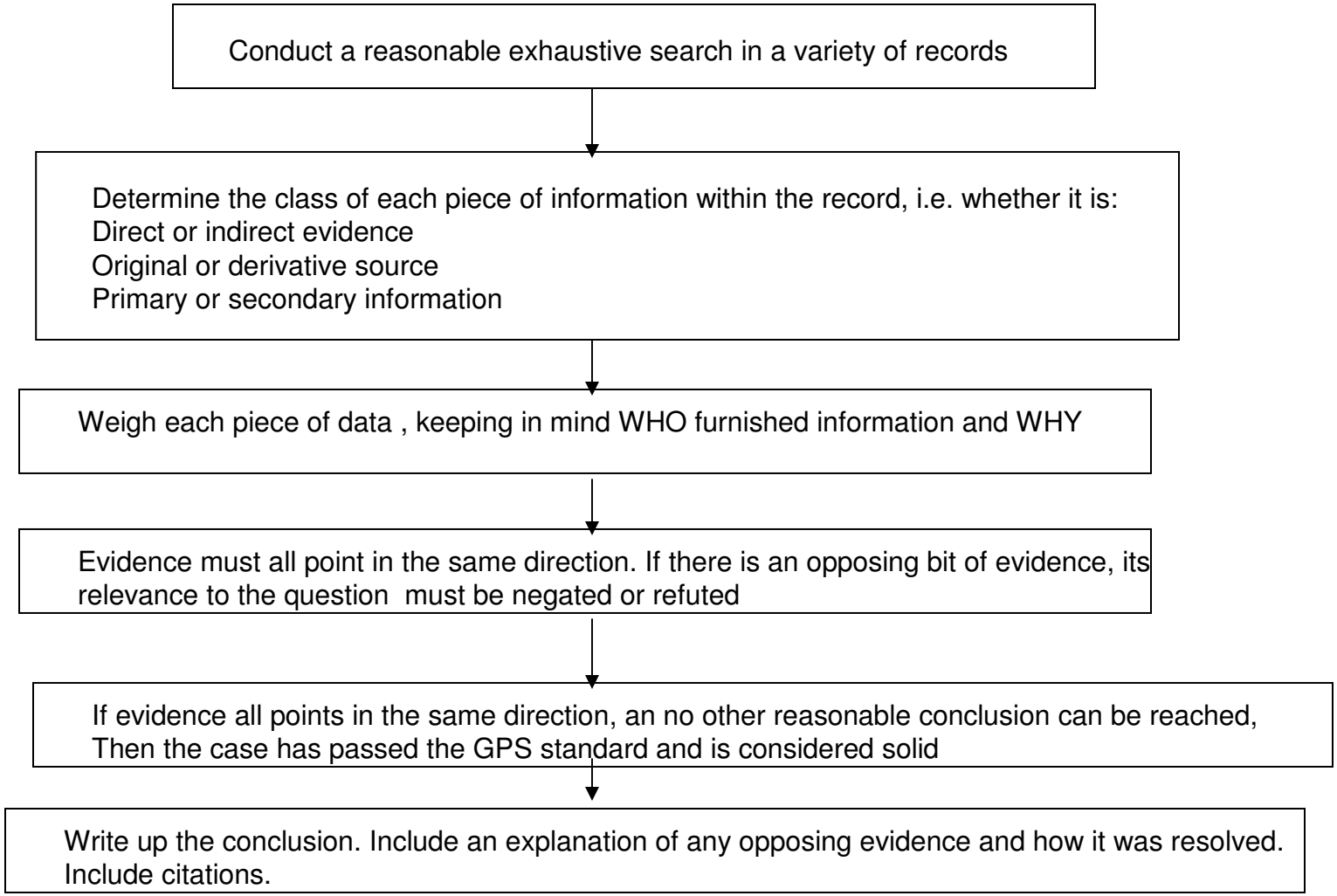
# What is Evidence ?

- Evidence is *anything* that supports certain claim
  - Not assumptions, clarification or other claims
  - Evidence is a record of something
- Evidence can be diverse (various things may be produced as evidence)
  - Documents as evidence
  - Testimony as evidence
  - Test results as evidence (someone has to make the verdict)
  - Measurement results as evidence
  - Process, product, people evidence
- Evidence uses heterogeneous formats
- Evidence needs to be interpreted
- Evidence needs to be evaluated
- Evidence needs to be managed
  - Evidence is stored in evidence repositories
- Argument structure determines what evidence is collected
  - Also argument criticality determines evidence "quality"
  - Evaluation of available evidence may require additional evidence

# Communities of interest



# GPS standard



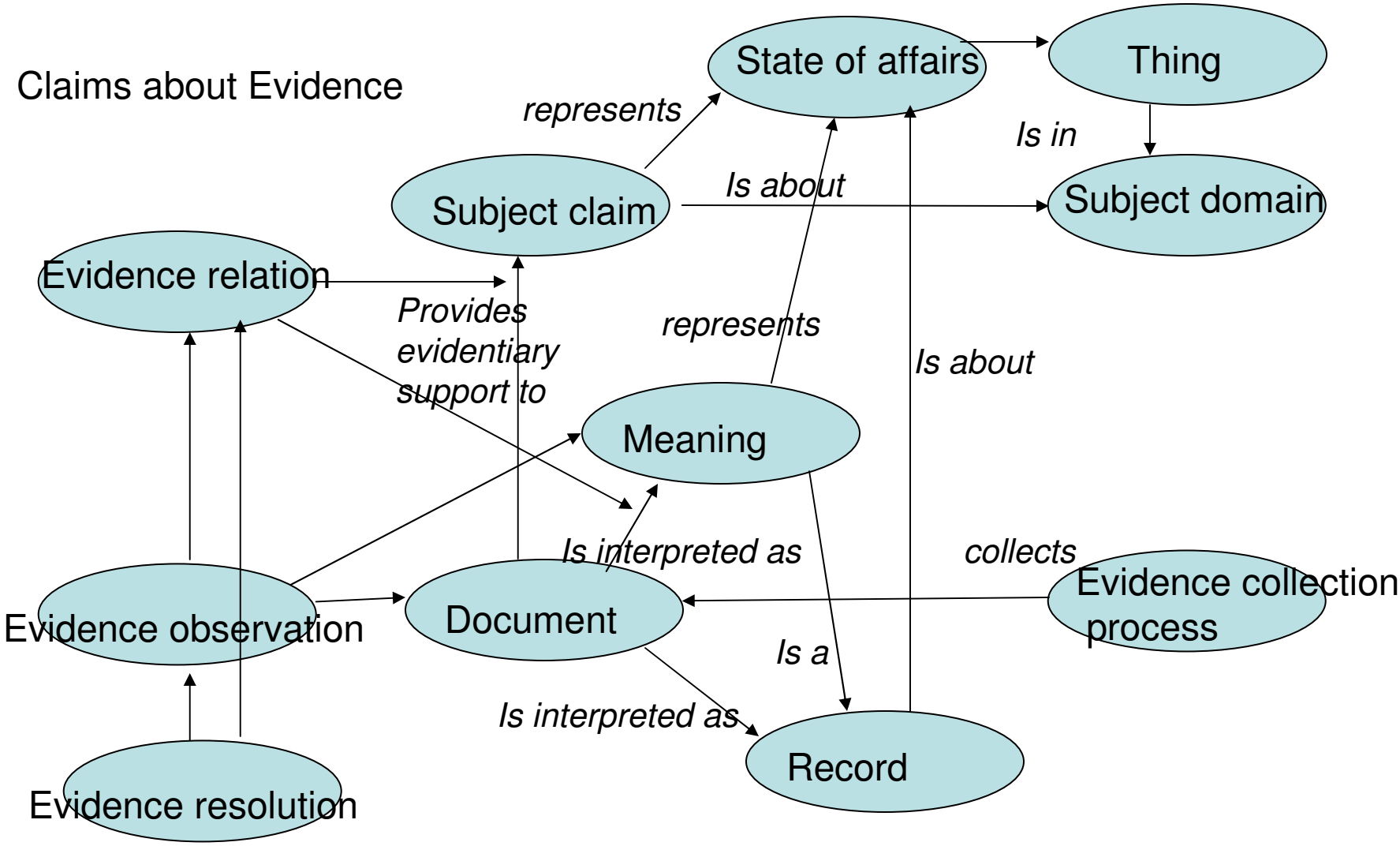
# Evidence metamodel

- *Vocabulary* for evidence collection projects, including
  - Management of evidence
  - Interpreting evidence
  - Evaluation of evidence
  - Exchange of evidence
- The evidence vocabulary describes *claims made about evidence*
  - Evidence vocabulary is reused in every argument for various diverse domains
  - Evidence arguments are reused
  - As opposed to subject domain claims and arguments, which are specific to each subject domain
- Interchange format for evidence (XSD schema)

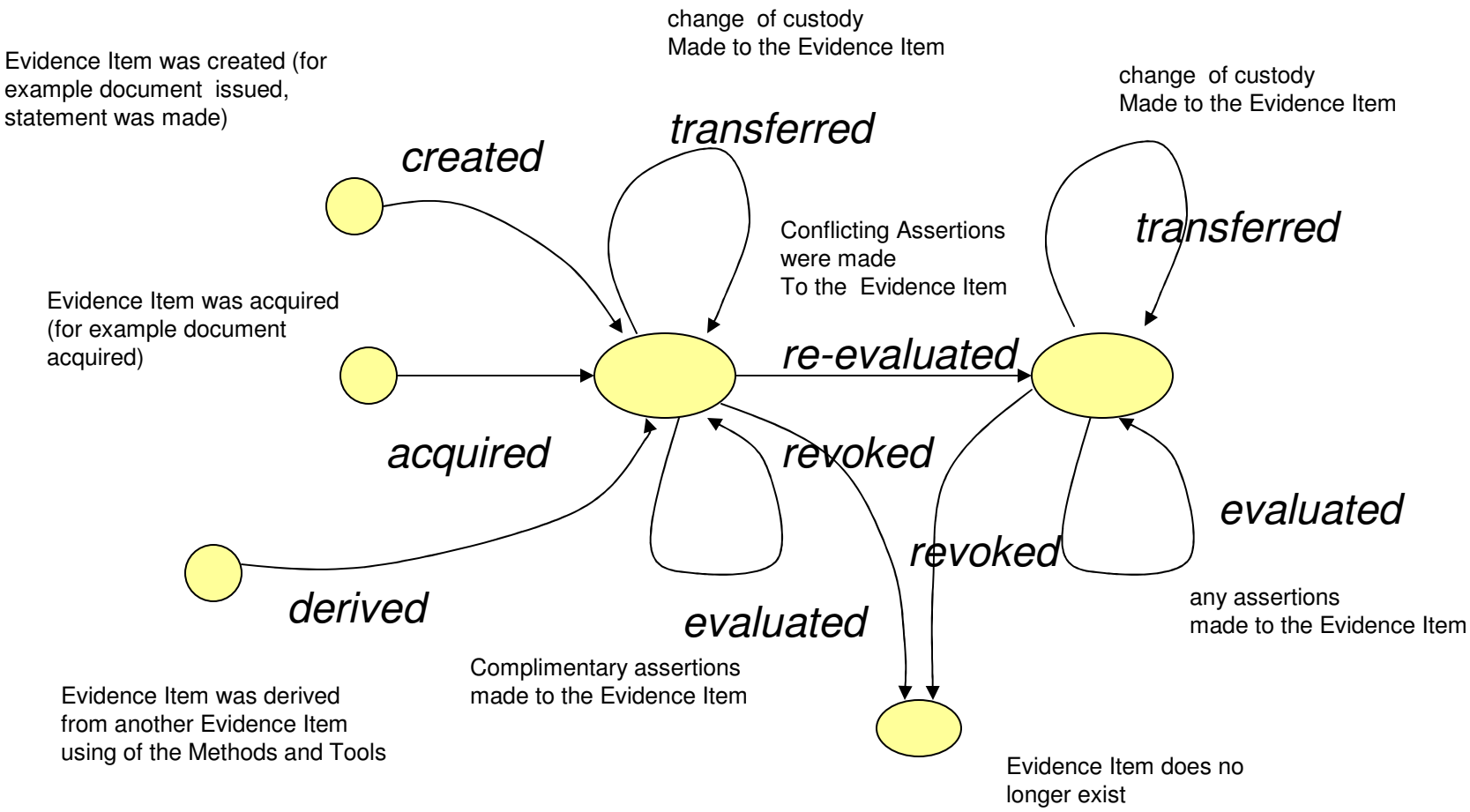
# Claims about evidence

- Evidence has provenance
  - Source
  - Who
  - When
  - Evidence collection involves certain processes (reviews, testing, analysis, etc.)
- Evidence has timing
- Evidence has meaning
- Evidence has “quality”
  - Direct or indirect
  - Primary or secondary
  - Document: original or derived
- Evidential support has
  - The entire evidence package needs to be evaluated
  - There are well-defined “Standards of proof”, such as
    - Clean and Convincing Evidence (CCE)
    - Preponderance of evidence (POE)
    - Genealogical Proof Standard (GPS)
    - Beyond the reasonable doubt (BRD)

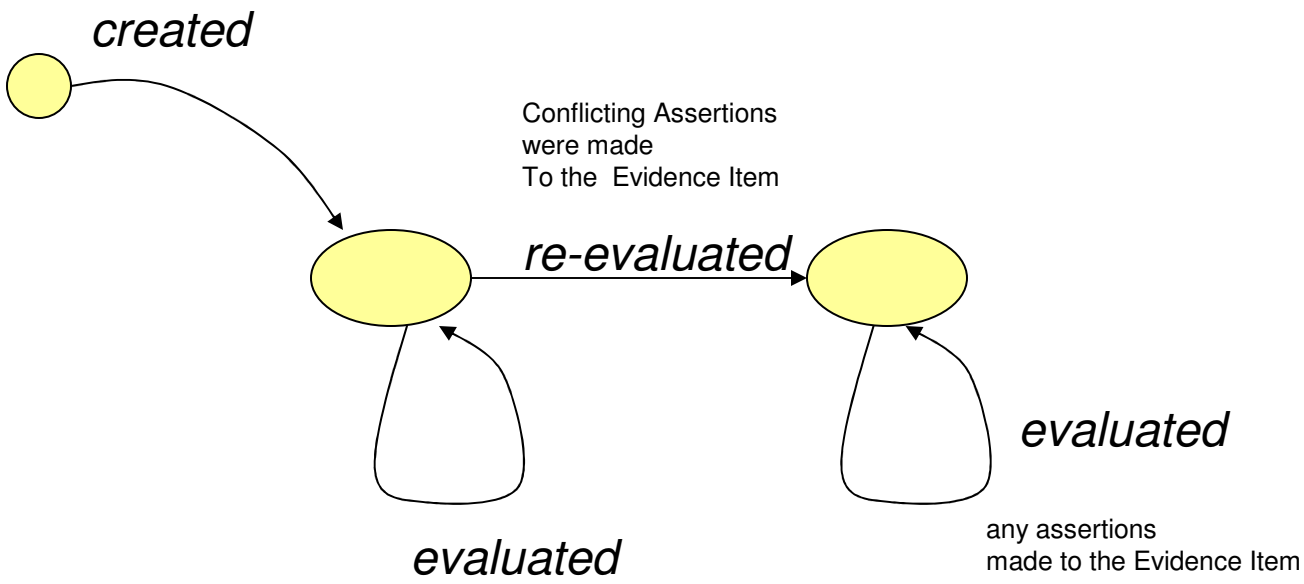
# The context for the evidence metamodel



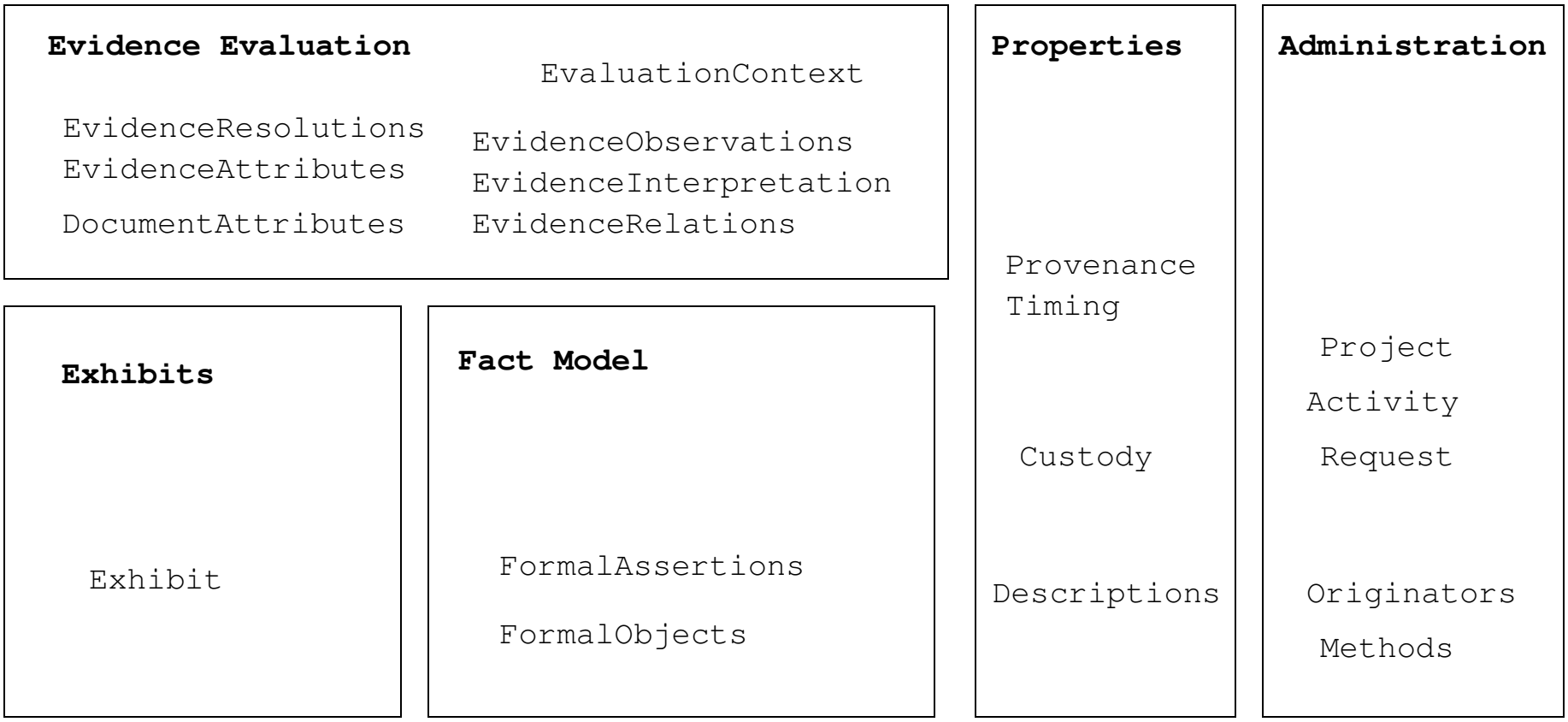
# Evidence Events



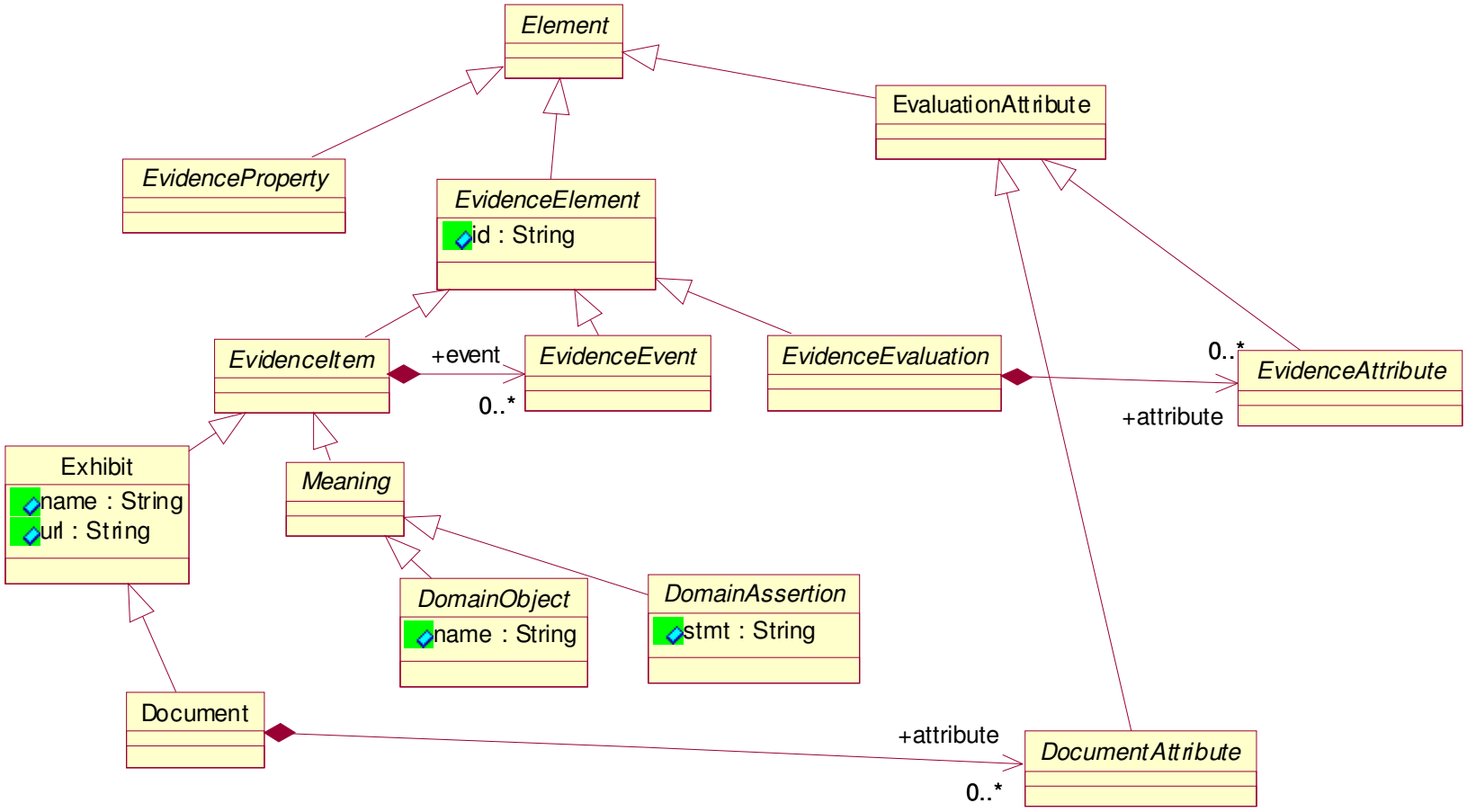
Evidence Item was created (for example document issued, statement was made)



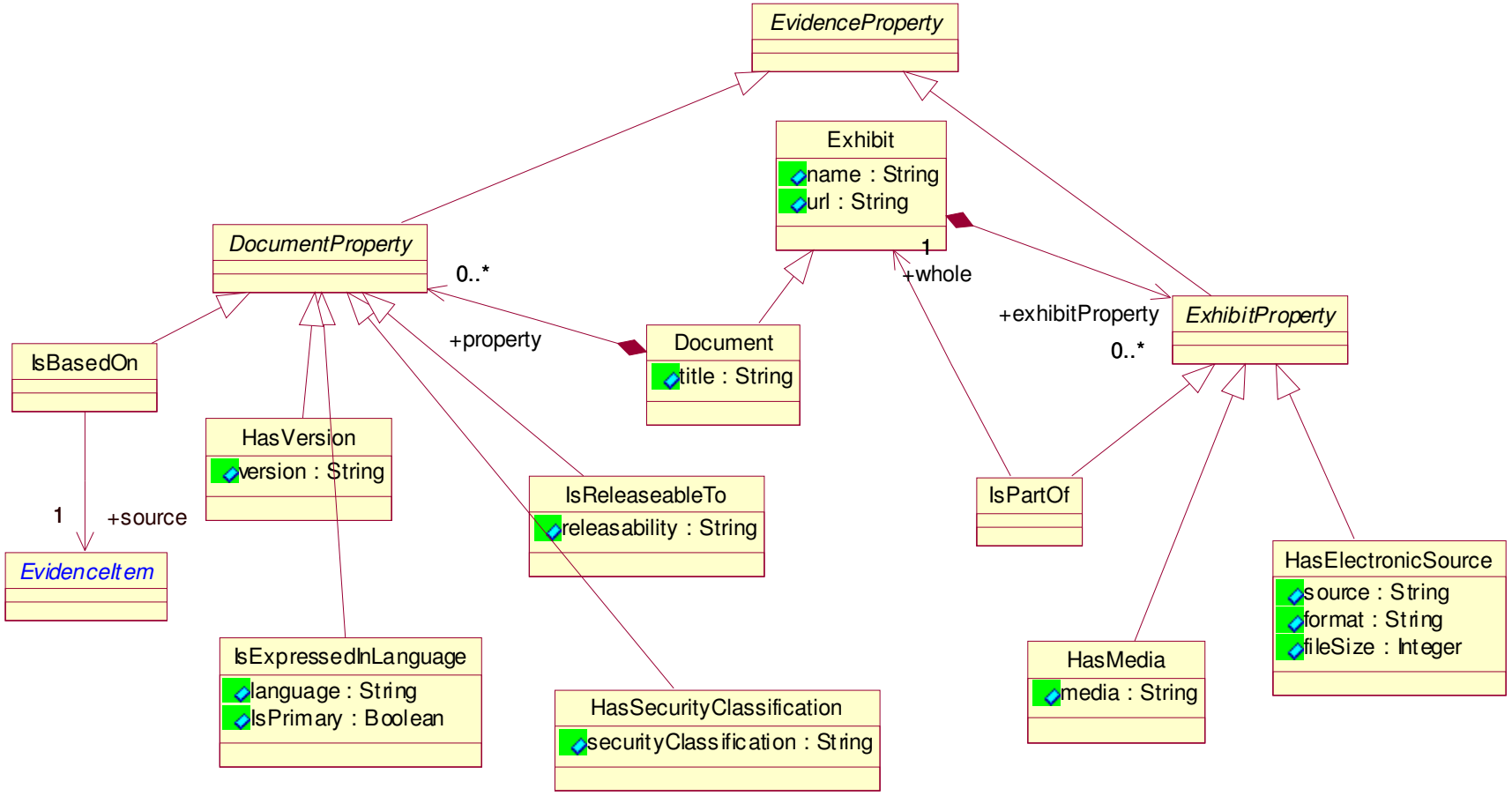
# Overview of SAEM



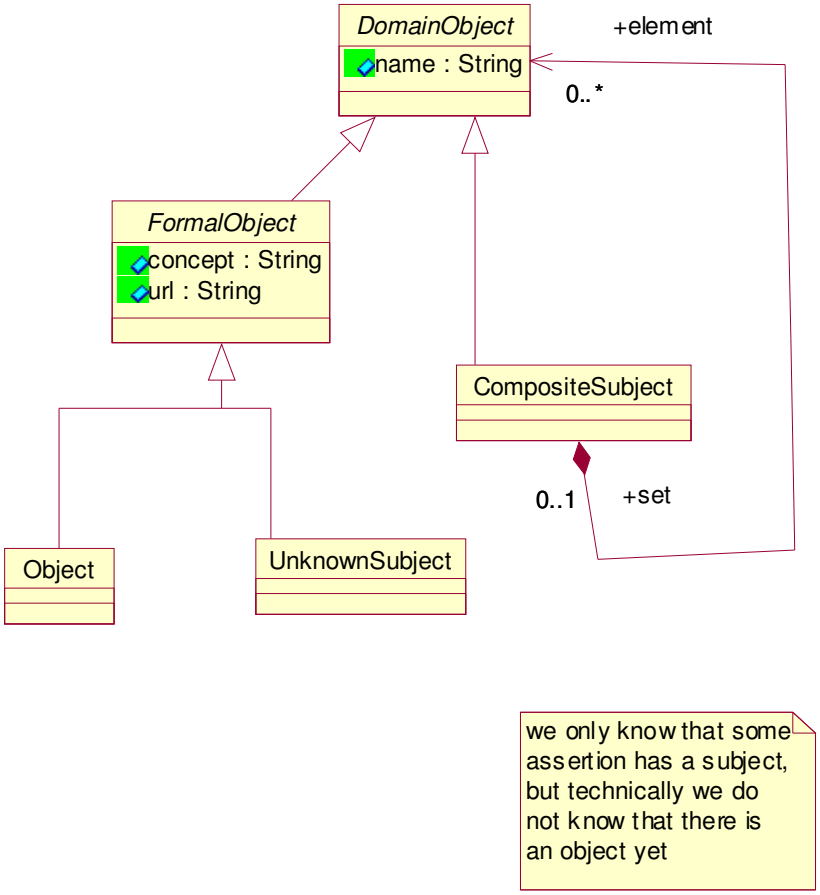
# Evidence Elements



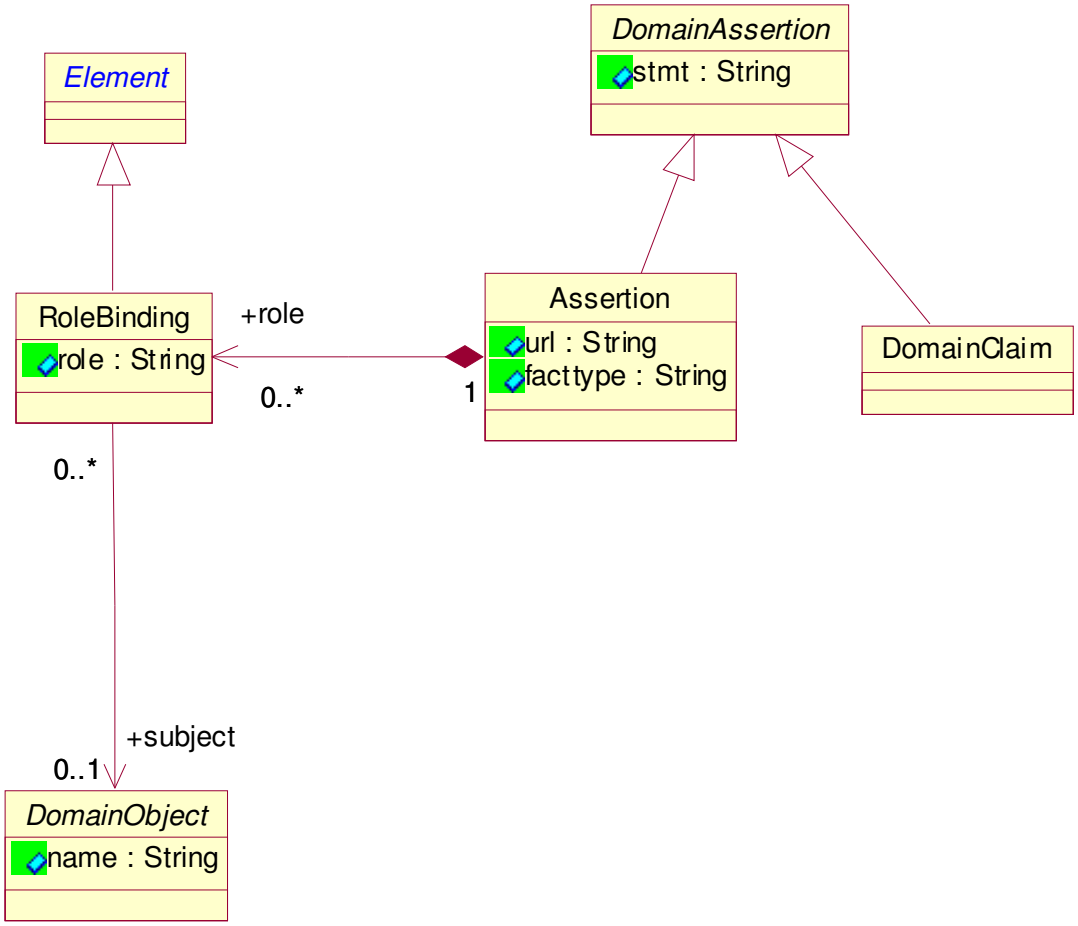
# Exibits



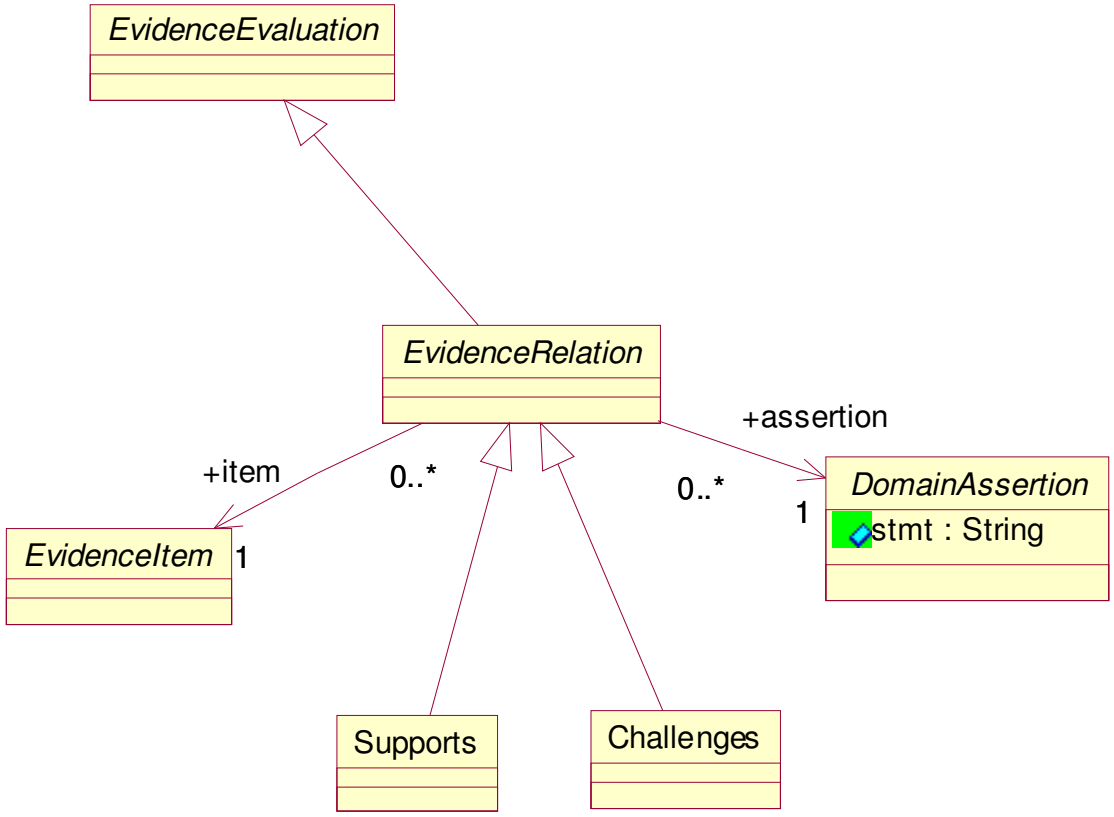
# Formal Objects



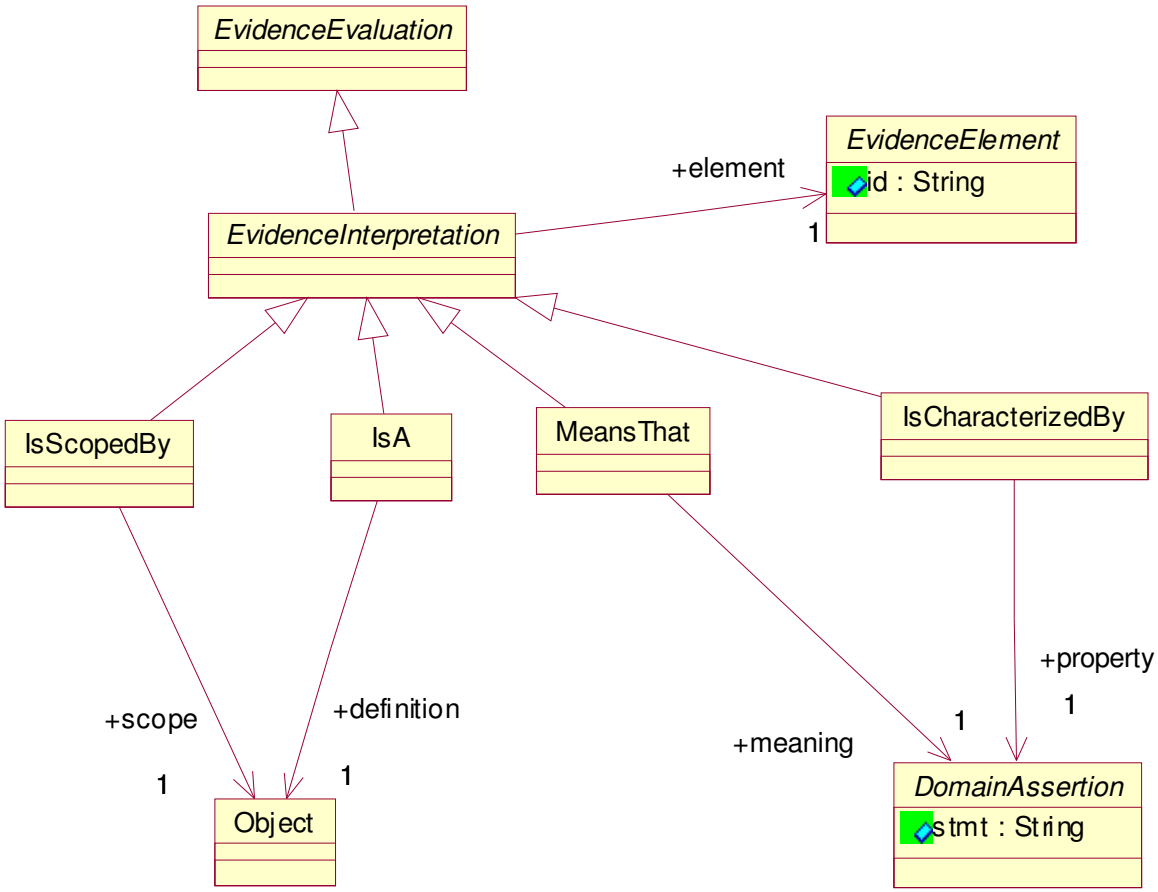
# Formal Assertions



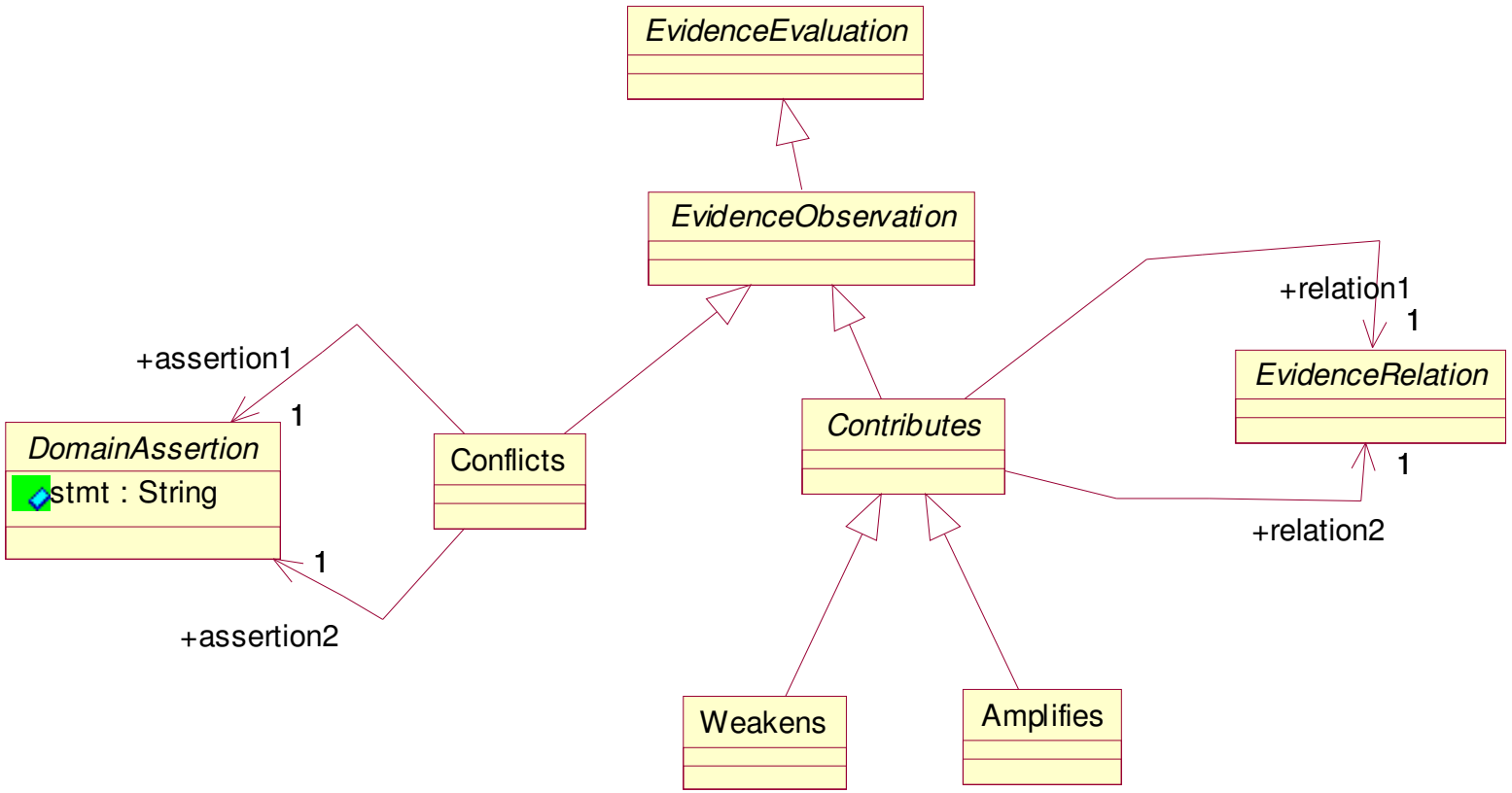
# Evidence Relations



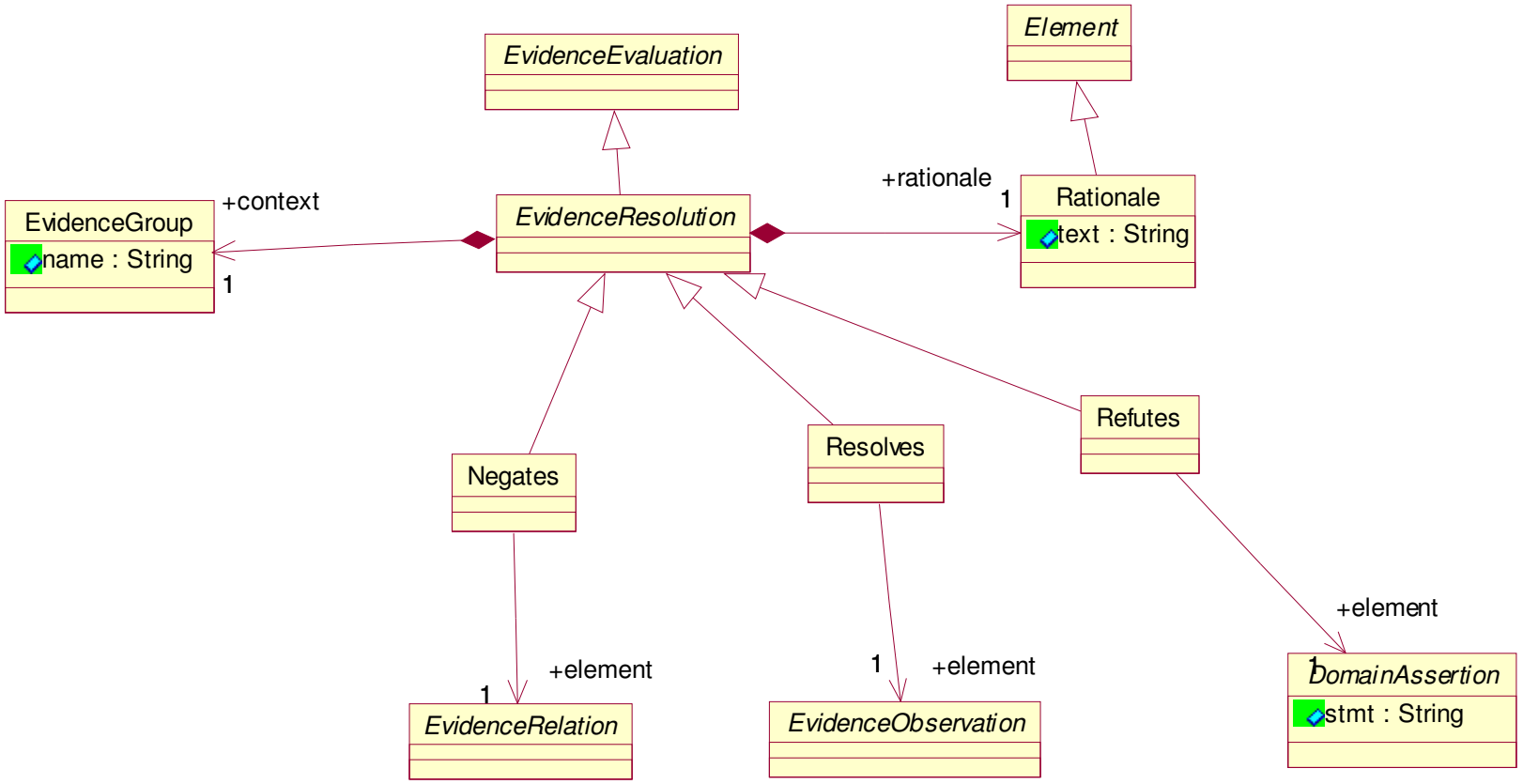
# Evidence Interpretation



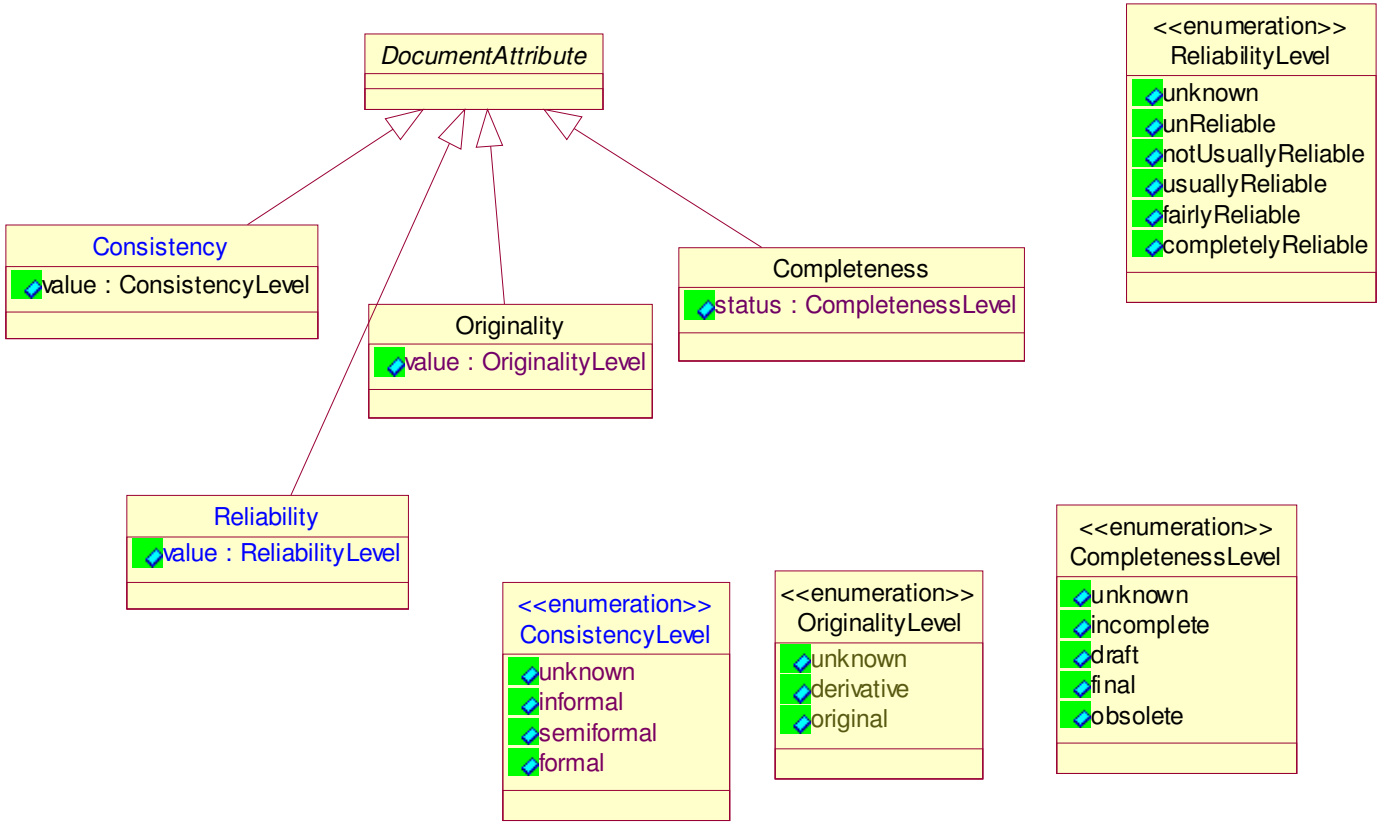
# Evidence Observations



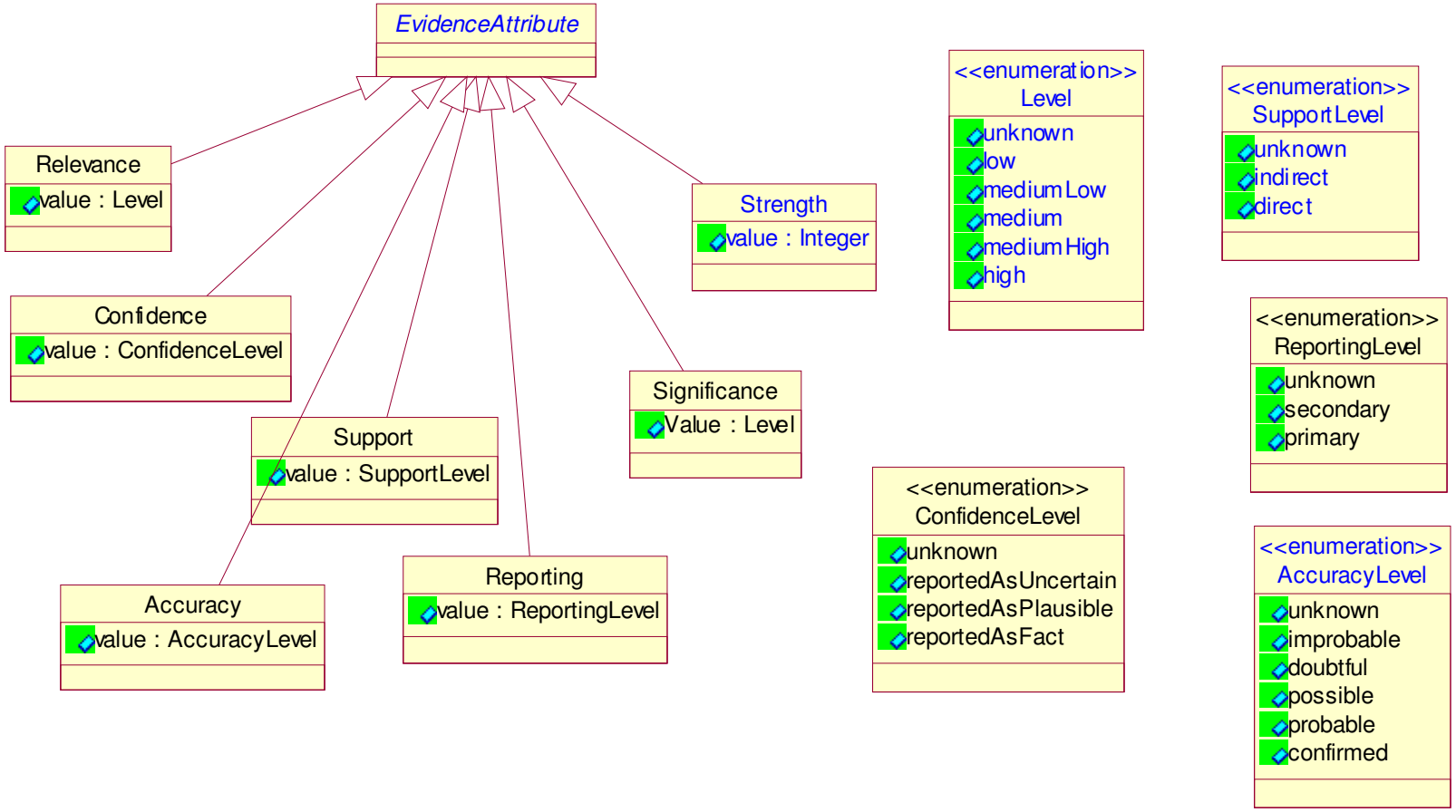
# Evidence Resolutions



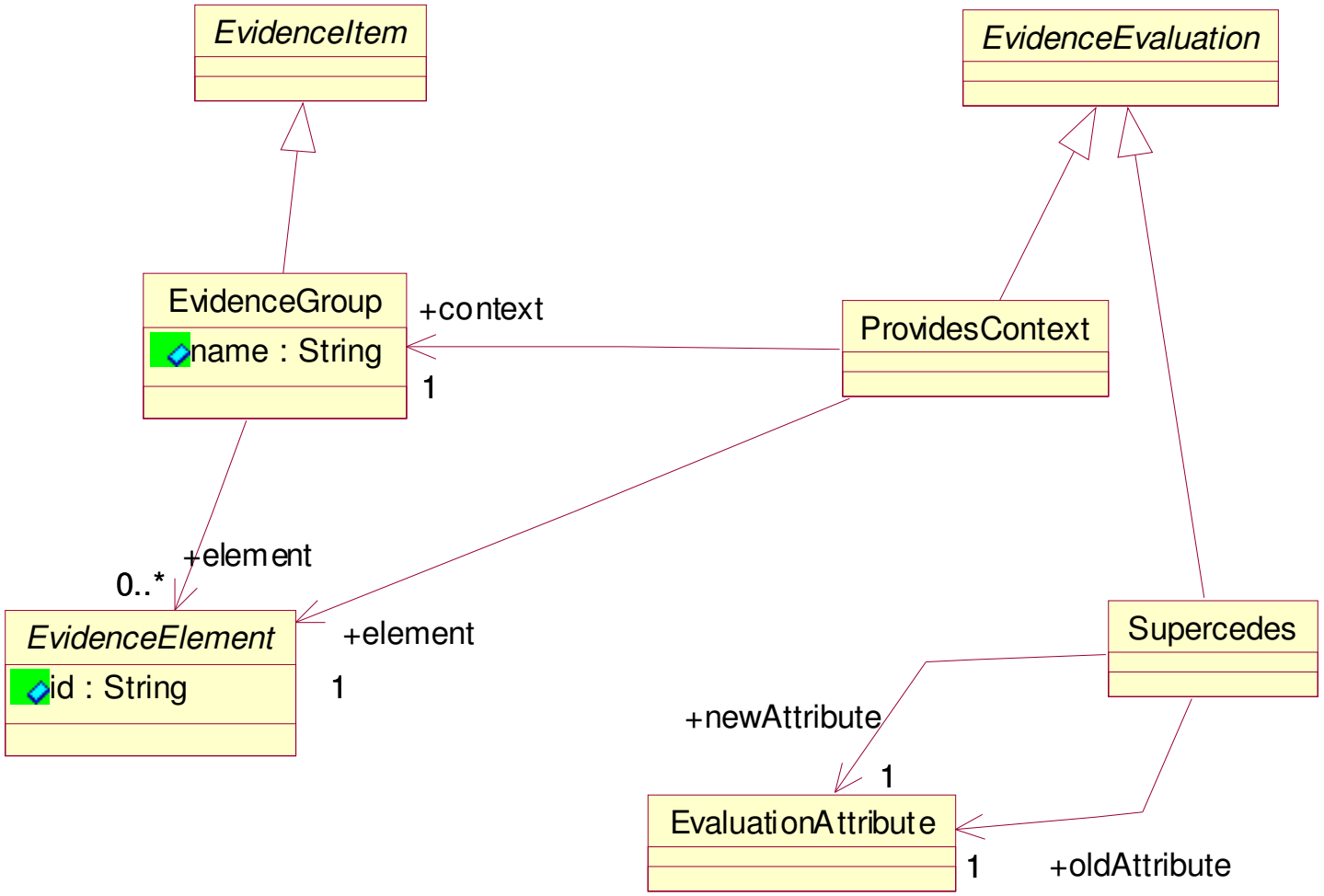
# Document Attributes



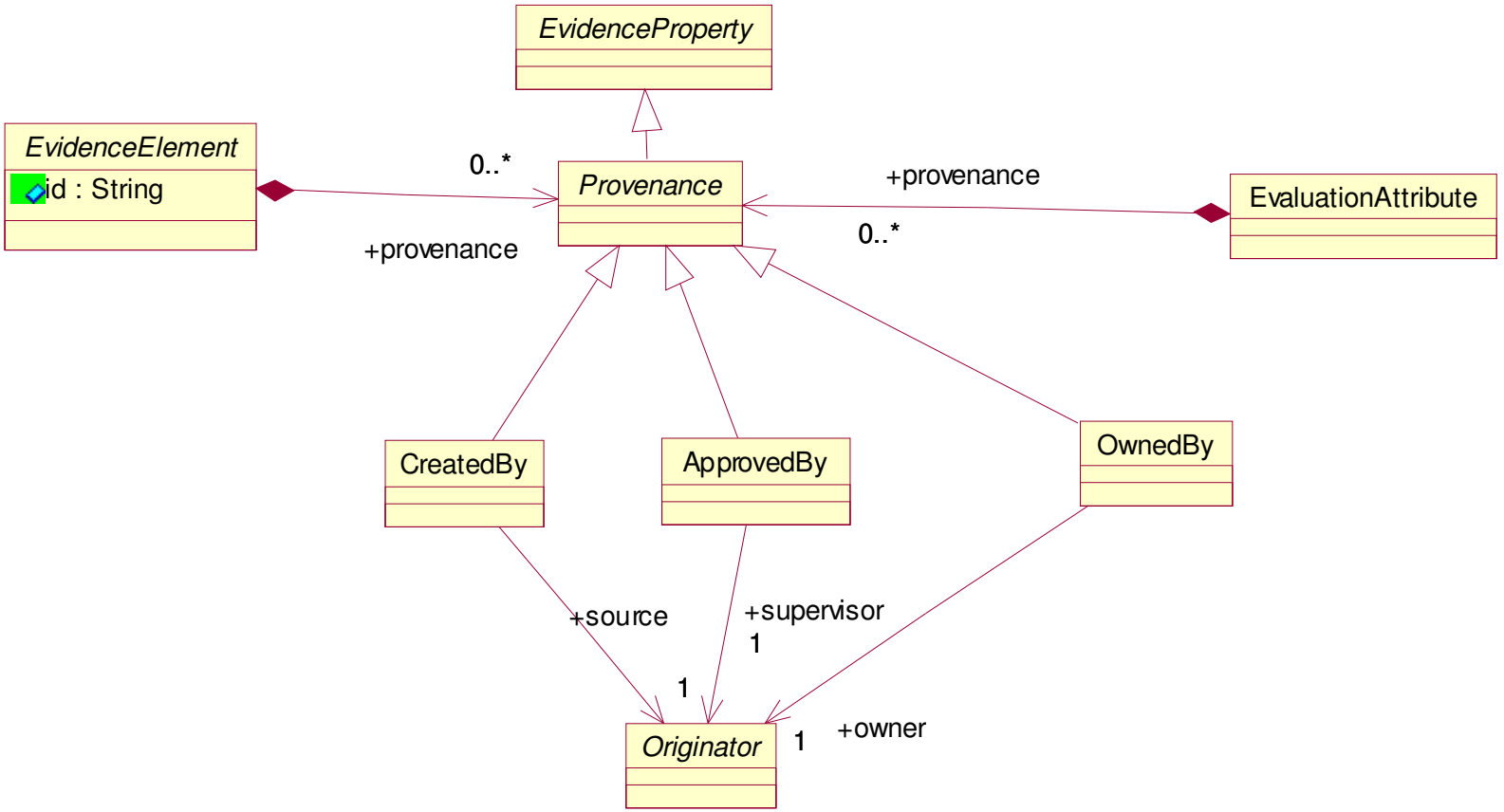
# Evidence Attributes



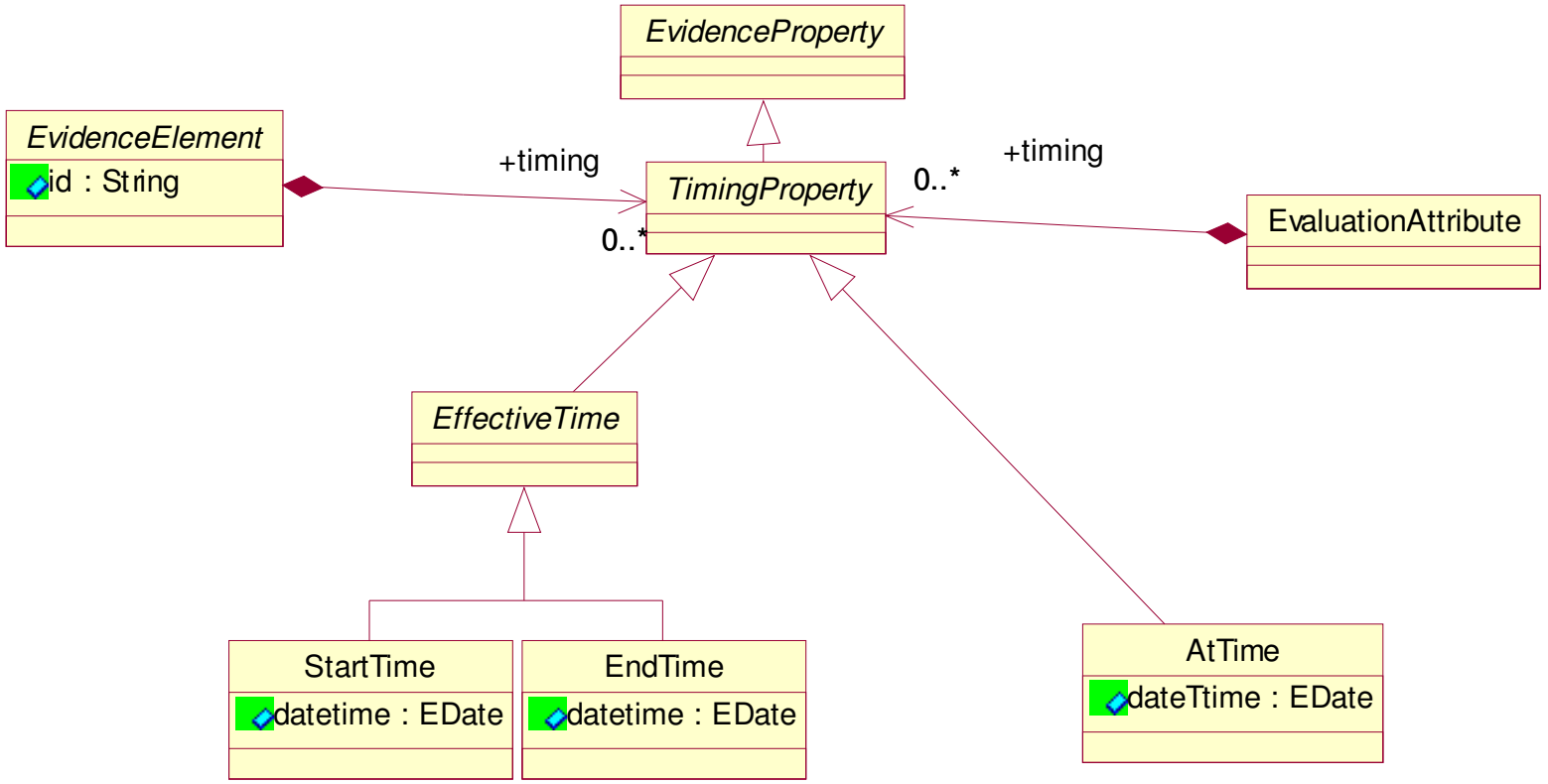
# Evaluation Context



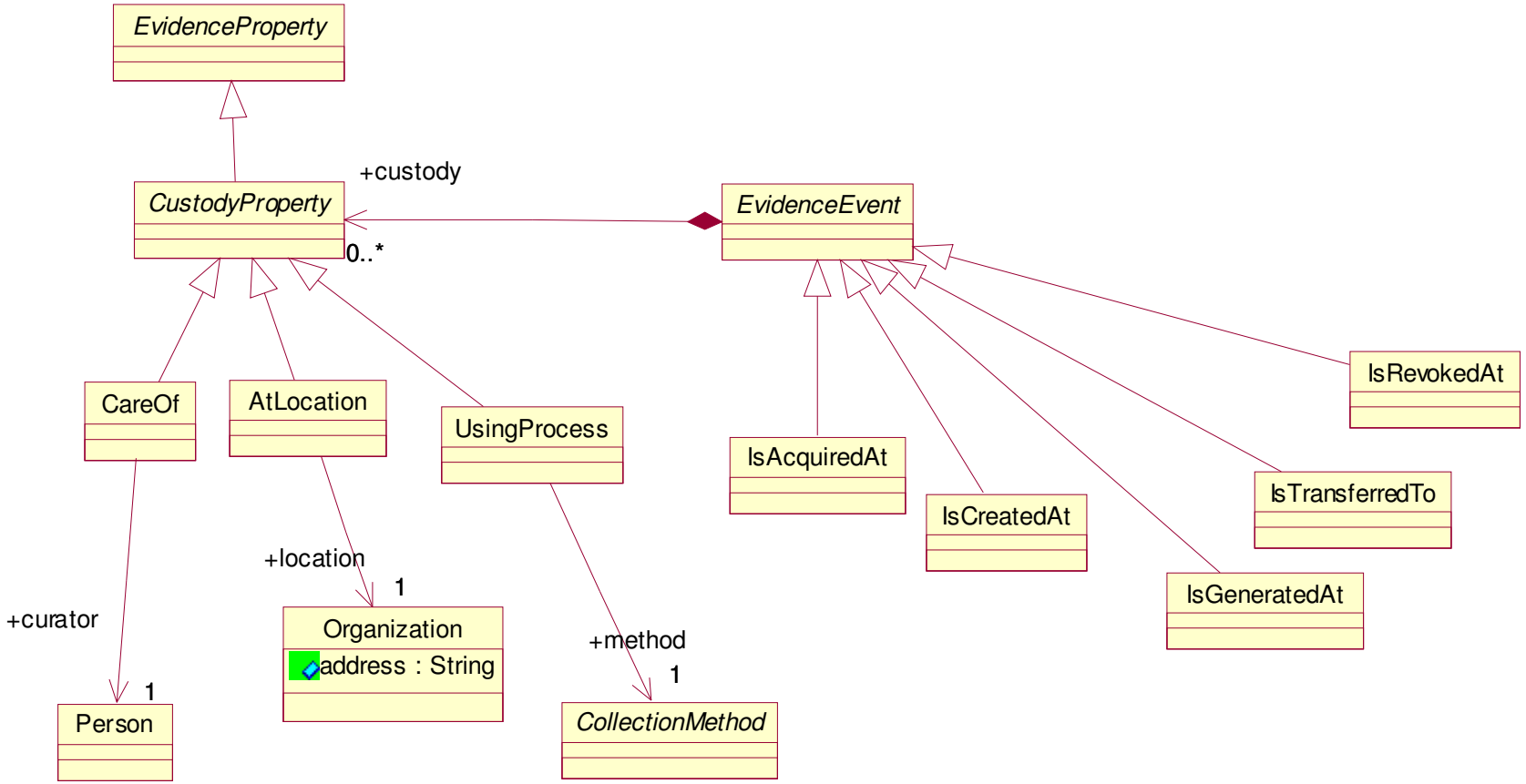
# Provenance



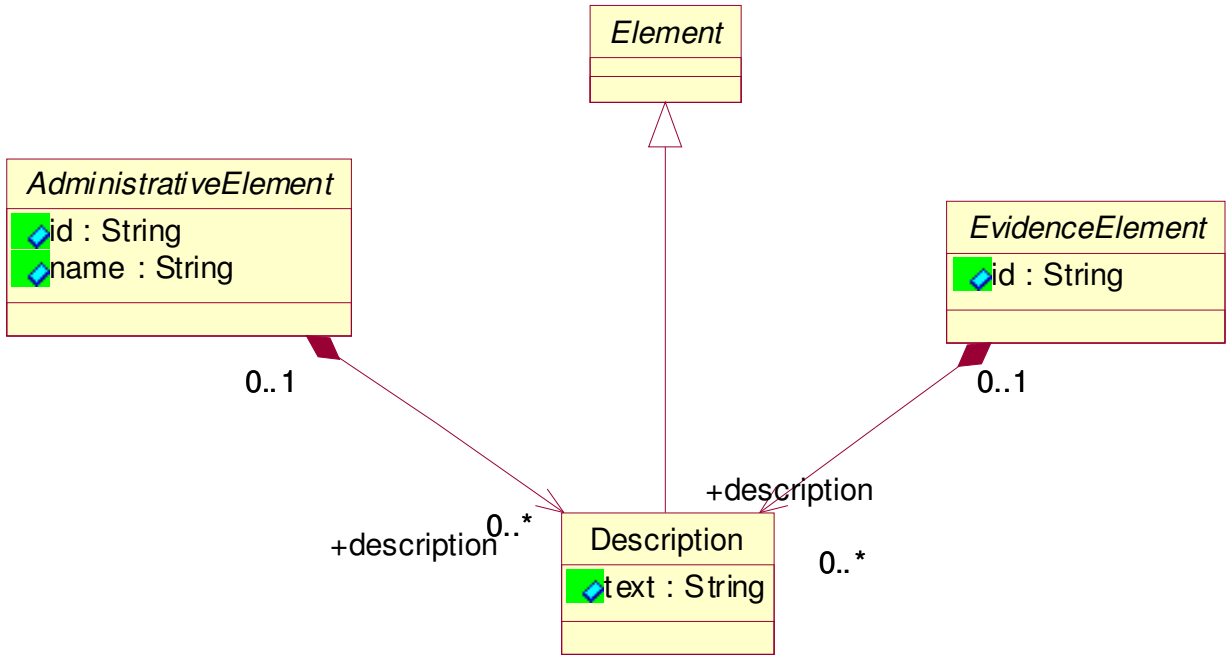
# Timing



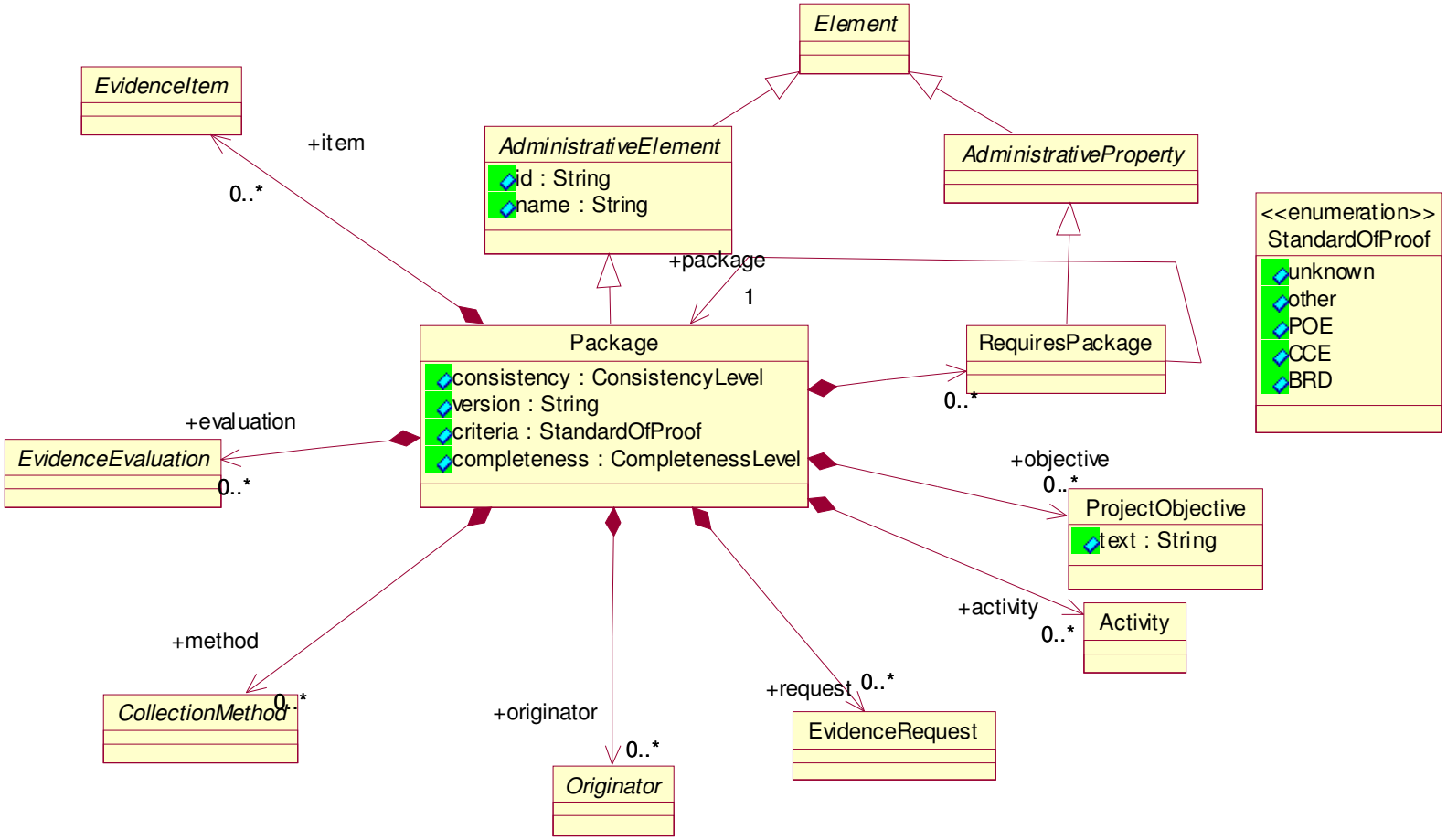
# Evidence Events



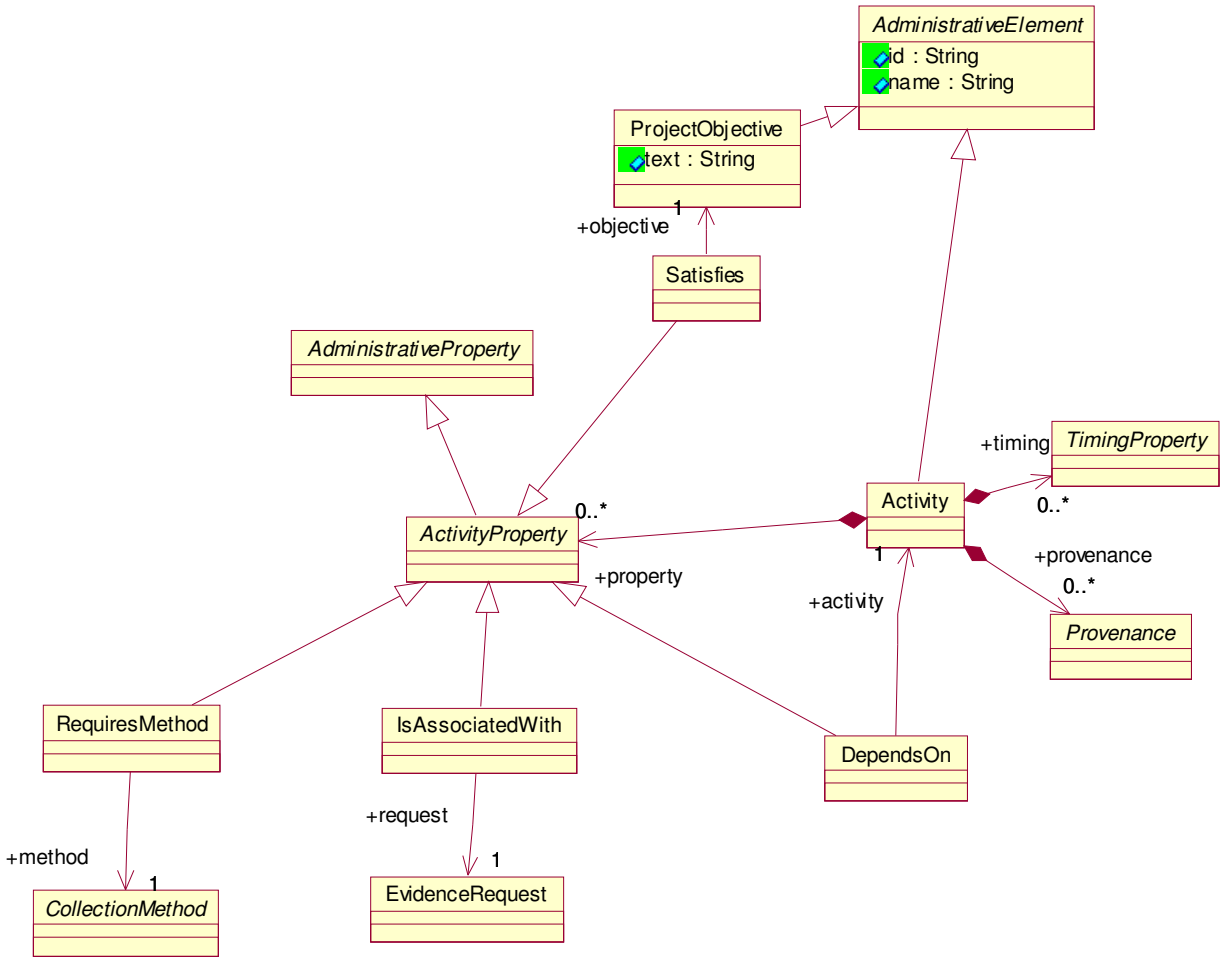
# Descriptions



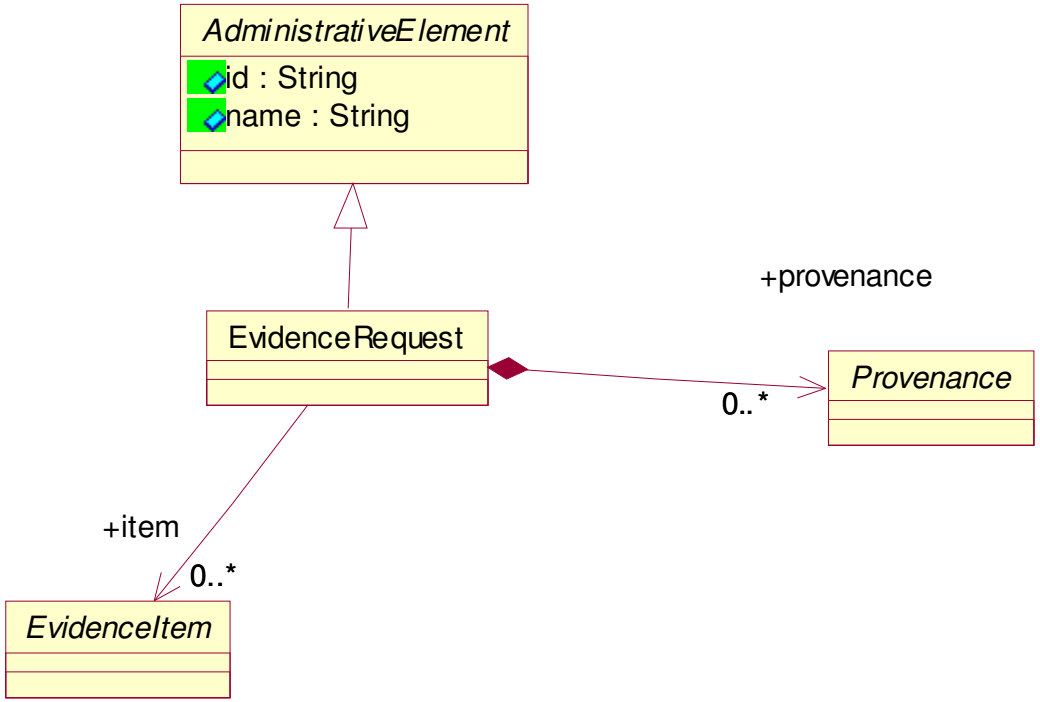
# Project



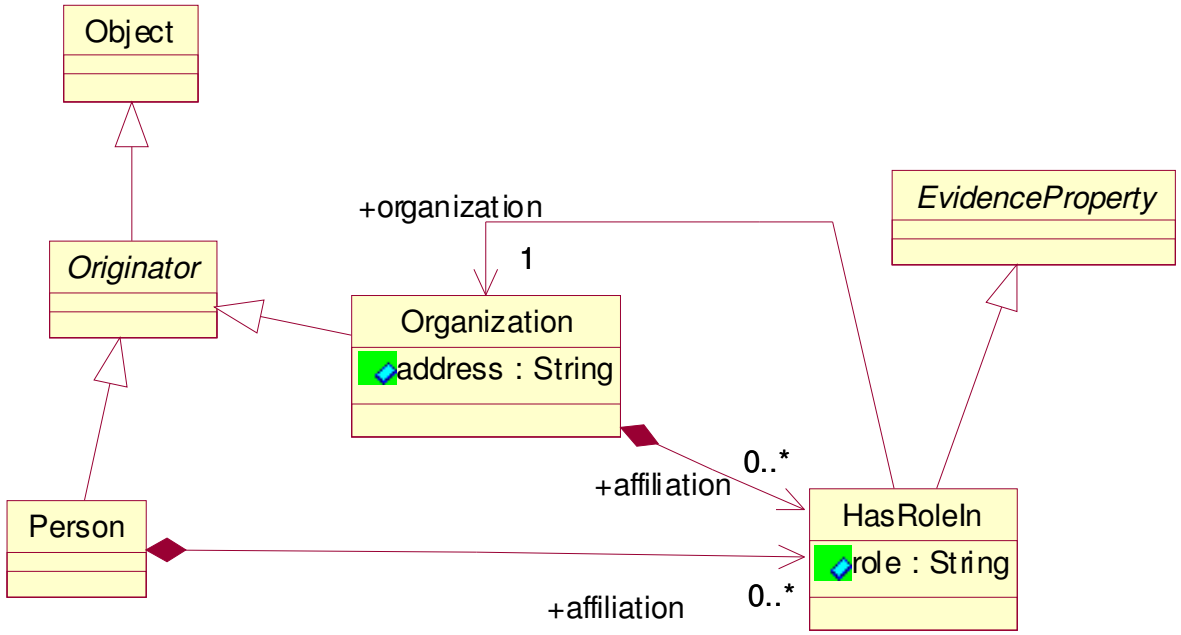
# Project Activities



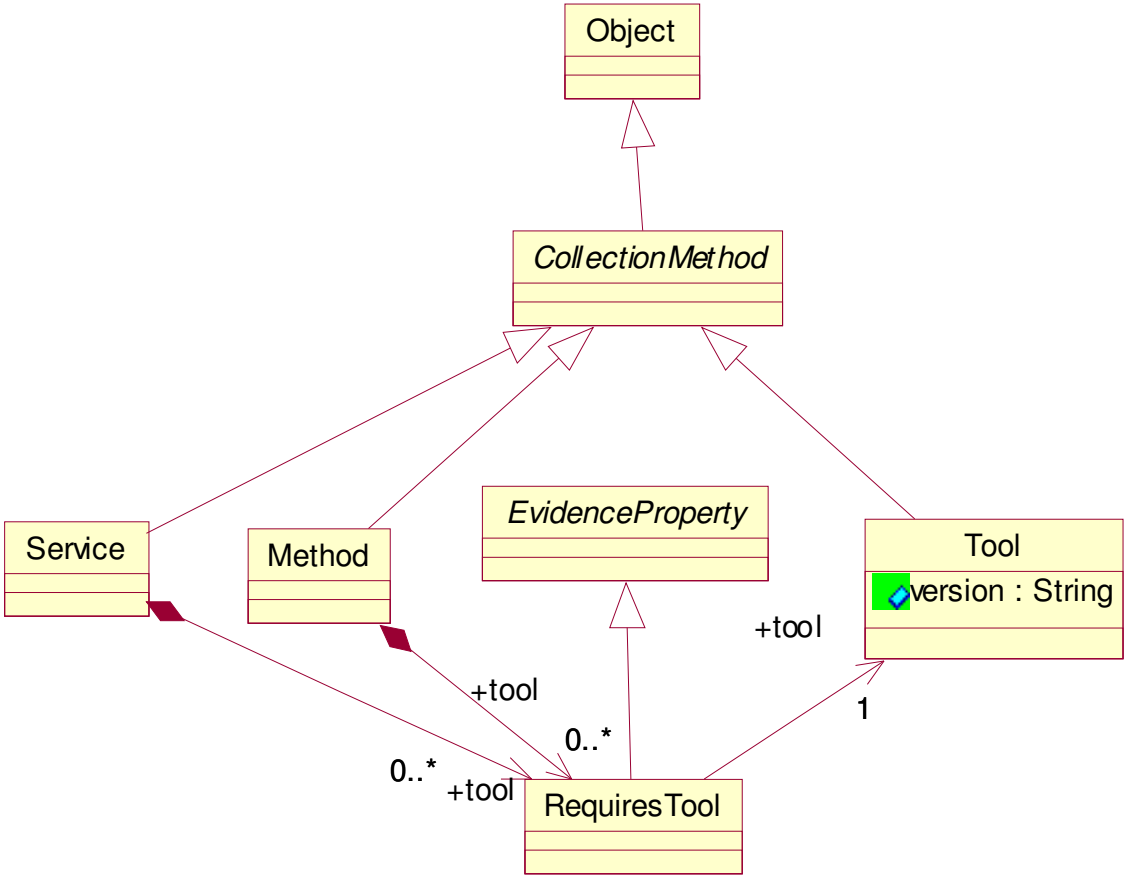
# Request



# Originators



# Methods



Questions ?