TrustCoM

Deliverable
15

Report on Legal Issues Appendix D

Conceptual Model for Legal Risk Analysis

WP9 Legal Issues

Tobias Mahler, Fredrik Vraalsen (eds.)

31 July 2005
Version 1.0

TrustCoM

A trust and Contract Management framework enabling secure collaborative business processing in on-demand created, self-managed, scalable, and highly dynamic Virtual Organisations

SIXTH FRAMEWORK PROGRAMME

PRIORITY IST-2002-2.3.1.9

Prepared for the European Commission under FP6 Contract No. 01945 as a deliverable form

Deliverable datasheet

Project acronym: TrustCoM

Project full title: *A trust and Contract Management framework enabling secure collaborative business processing in on-demand created, self-managed, scalable, and highly dynamic Virtual Organisations*

Action Line:	**6**
Activity:	**6.2**
Work Package:	**9**
Task:	**6.2.1**

Document title:	D 15 Appendix D
Version:	1.0
Document reference:	N/A
Official delivery date:	31 July 2005
Actual publication date:	
File name:	
Type of document:	Report
Nature:	Public

Authors:	Jon Bing[1], Andrew Jones[2], Mass Soldal Lund[3], Tobias Mahler[1], Thomas Olsen[1], Xavier Parent[2], Ketil Stølen[3], Fredrik Vraalsen[3]
Reviewers:	CCLRC and Atos Origin
Approved by:	

---

[1] NRCCL

[2] KCL

[3] SINTEF

Table of Content

1 Introduction

In the context of legal risk analysis, we aim at producing models of instances of risks, i.e. the outcomes of risk analyses. However, people differ in their understanding of, e.g., the concept “risk”, and there is a danger that the risk models will be inherently ambiguous. For this reason we see the need for drafting a conceptual model which defines the concepts in our universe of discourse. With such a conceptual model in place, the process of making risk models entails coupling instances in the real world with the concepts defined in the conceptual model. The outcome should then be less ambiguous, compared to using the concepts floating around in people’s heads. In this chapter we present the conceptual model for legal risk analysis that we have developed. This model forms the basis for the following chapters.

We define conceptual model to be the same as an ontological model, i.e. we relate it to philosophical ontology. These terms are defined as [4]:

- An ontology is those things in the world whose existence a theory commits to
- An ontological model is a model of these things (and their relations)

Figure 1 shows one example of the conceptualization process we have used. In the real world there exist things and concepts, where concepts represent classes of things. For example, the concept “tiger” is the class of all actual tigers. In addition, a tiger may be considered a risk and is thus contained in the concept risk (the class of all risks).

[4] Partridge, C., Setting the Scene. Introduction to ECOOP 2004 – WS6, Philosophy, Ontology, and Information Systems, 2004.

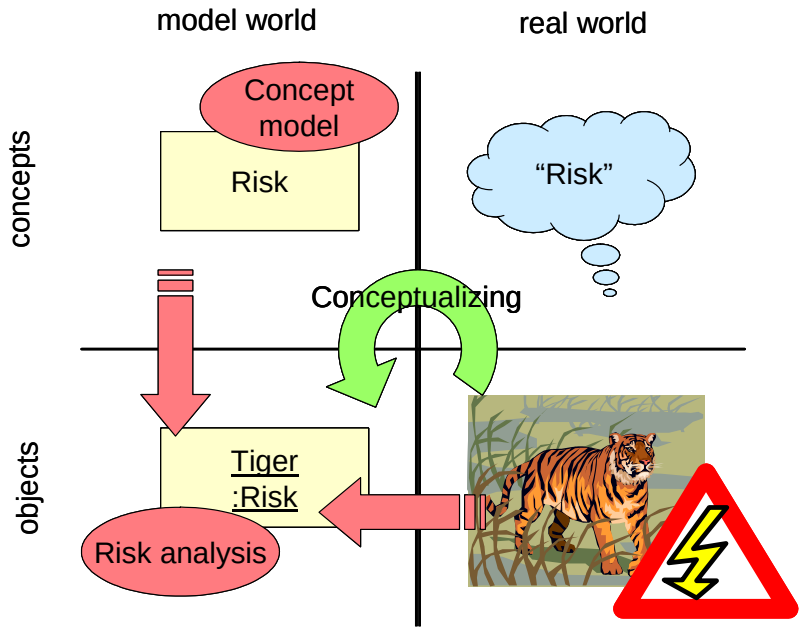

Figure 1: Conceptualization process

Our conceptual model for legal risk analysis is described using the Unified Modeling Language (UML)[5]. Section 2 explains the various facilities of UML that were used in creating the model. Sections 3 thru 8 introduce the various parts of the model individually. Finally, the combined model is presented in section 9.

2 Conceptual Models Using UML Class Diagrams

We have used UML class diagrams to create the conceptual model. This section gives a brief introduction to the elements of UML class diagrams used to model the concepts and their relations. For further details on UML, we refer to [5] and [6].

A class diagram describes the *types* of objects (classes, concepts) in the system (universe of discourse) and the various kinds of *relationships* that exist among them. In our case, we use a class to represent a concept. Classes are represented using rectangles containing the class name, as shown in Figure 2.

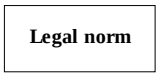

Figure 2: Class example

There are two principal kinds of relationships between classes:

- **associations** – relationships between *instances* of classes/concepts, e.g. a legal norm consists of an antecedent and a consequent
- **subtypes** – generalisation relationships between the classes/concepts themselves, e.g. contract is a kind of legal text

These are described in more detail below.

2.1 Associations

Associations are either binary (relationship between two classes) or n-ary (relationship between multiple classes). A binary relationship is shown as a line connecting the two classes/concepts in the relationship. An n-ary relationship is represented as a diamond shape with lines connecting it to each of the classes/concepts in the relationship. Each end may be labelled explicitly with a role name. If the role name is left out, the class name is typically used as the role name. The association itself may also be given a name to describe the type of relationship. This name is written in italic.

An association end may also have a multiplicity or cardinality, indicating how many instances of the class/concept may be involved in the relationship. Multiplicity indicates lower and upper bounds for the number of instances, e.g. *2..4*, with * representing any number. If a single number is used, the lower and upper bounds

[5] Rumbaugh, J., Jacobson, I., and Booch, G., The Unified Modeling Language Reference Manual, Addison-Wesley, 1999.

[6] Fowler, M., UML distilled: a brief guide to the standard object modeling language, Addison-Wesley, 2000.

are equal, whereas the * by itself represents the range *0..n,* where *n* is an arbitrary large natural number. The default multiplicity if one is not explicitly given is 1.

The example in Figure 3 shows the two classes Parent and Child and the father-daughter relationship. A father can have zero or more daughters, represented by the *, whereas each daughter has exactly one father.

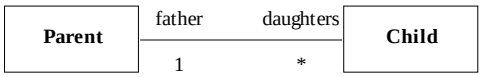

Figure 3: Association example

UML contains two special association types, aggregation and composition. Aggregation is the *part-of* relationship, e.g. an engine and wheels are part of a car. An aggregation is represented using an open diamond shape at the association end of the class that contains the parts, as shown in Figure 4. Composition is a stronger variety of aggregation, where the parts "live and die" with the whole. It is represented in the same way as aggregation but using a black diamond shape.

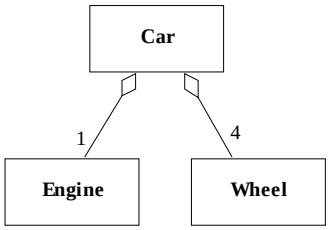

Figure 4: Aggregation example

If an association has special attributes, it is possible to model this by attaching a class to the association. This is called an association class, and is shown by attaching a class to an association using a dashed line, as seen in e.g. Figure 7 which shows an n-ary relationship connected to an association class (Circumstance)**Error! Reference source not found.**.

2.2 Subtypes

To give an example of subtyping, we can say that Contract is a subtype of Legal text if all instances of Contract are also instances of Legal text. The key is that everything we say about the superclass (Legal text), such as associations to other classes, is true also for the subclass (Contract). Subtypes are modelled using arrows, as shown in Figure 5.

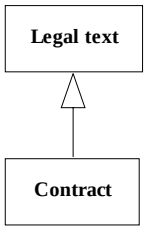

Figure 5: Subtyping example

3 Legal Norms

Central to legal risk analysis are **legal norms**, which describe legal requirements and consequences. Legal norms have the general structure of an **antecedent** and a **consequent**:

if [A] then [B]

The antecedent describes the **criteria**, i.e. which factual **circumstances** have to be present, for the norm to fire. The consequent indicates the **effect** of the norm being applied. The effect may be a link to further norms to be applied, which taken together will represent the norms governing the case at hand. When law is applied to a case or situation, the legal requirements have to be compared with the factual circumstances of the case. Figure 6 shows a UML diagram depicting the concepts outlined in bold above and the relationships between them.

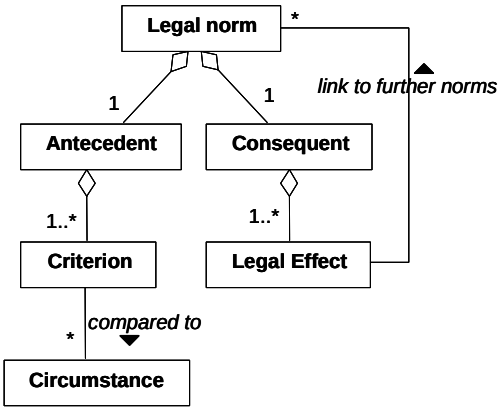

Figure 6: Conceptual model of legal norm

4 Actor and Circumstance

An **actor** is a natural person, i.e. a human being, a juristic person, e.g. an organization, or other types of behavioral entities, e.g. a software agent. The legal effect a particular norm has on an actor depends on the circumstances, as described above. A circumstance includes an actor, the **activity** being performed, as well as the **role** that actor plays while performing the activity, e.g. student, employer, (system) owner, etc. Further **entities**, e.g. persons, objects, and so on, may also be involved in the activity. For example, a circumstance may be that a person (*actor*) who is an employee of company A (*role*) accesses (*activity*) some information (*entity*) which belongs to company B. Figure 7 shows these concepts and relationships related to circumstance.

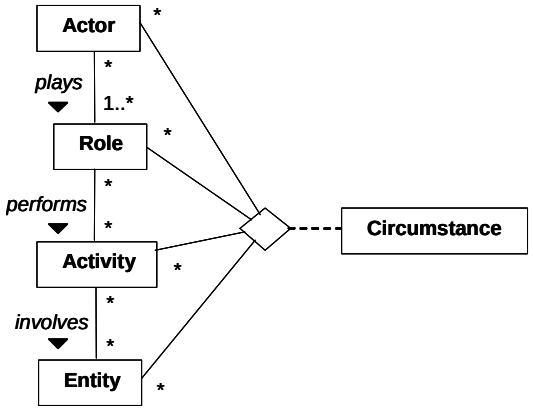

Figure 7 Circumstance

In general, an actor may play several roles and perform many activities, each involving a number of other entities. However, by looking at each combination of these as separate circumstances, this allows us to assign different legal effects to each circumstance. For example, the person in the example above may be permitted to access the information in that particular scenario, whereas another person employed by company C may be forbidden to access the same information.

5 Normative modalities

Legal norms are special in the sense that they bind the person or actor to certain behaviour through **obligations**, **prohibitions** and **permissions**. **Normative modalities** are used in deontic logic to describe the normative status (*permitted*, *obligatory*, *forbidden*, and so on) assigned to a state of affairs *A*[7]. *Obligation* may be expressed as O*A*, meaning "it is obligatory that *A*." The agency operator, E_i, is used to express propositions such as OE_iA, meaning "agent *i* is obliged to bring it about that *A*"[8]. *Permission* is the dual of obligation, i.e. $PE_iA = \neg O\neg E_iA$ ("agent *i* is permitted to bring it about that *A*"), and *prohibition* (forbidden) is simply the negation of permission, e.g. $\neg PE_iA$ ("agent *i* is forbidden/not permitted to bring it about that *A*").

We **assign** normative modalities to the relationship between legal effect and circumstance, as defined above, to specify which circumstances are permitted, obligatory and forbidden by the legal norm in question, as depicted in Figure 8.

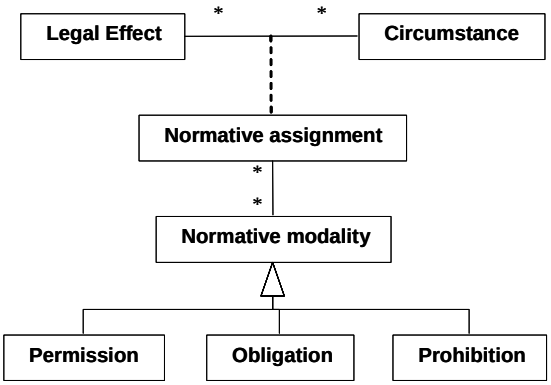

Figure 8 Normative modalities and effects of legal norms

The legal criteria are derived from legal reasoning based on the relevant source material, which may include statutes, regulations, court or administrative decisions, etc. The identification of such sources itself is an essential part of a legal decision making process. Figure 9 shows an example of some legal sources.

[7] Chellas, B. F., Modal Logic – An Introduction, Cambridge University Press, 1980.

[8] Elgesem, D., The Modal Logic of Agency, Nordic Journal of Philosophical Logic, vol. 2, 1997.

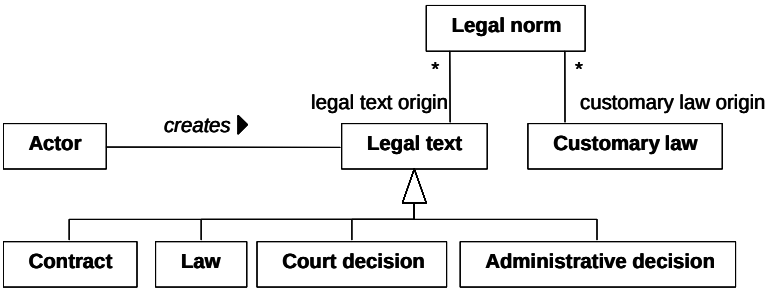

Figure 9: Legal source material

Comment [fvr1]: I've removed the figure as authorisation, power and right are no longer part of the combined conceptual model, but I think we can leave the discussion

6 Refinement of Normative Modalities

In section 5 we distinguish between the normative modalities obligation, prohibition and permission. *Authorisation* might be a better term than permission, since the first can be further divided into *power* and *permission*, with *right* as a subtype of permission.

Permission is the simplest: I have a permission to do something if I have no obligation not to do it.

Power conferring rules may admittedly be partly understood as permissive norms. However, it is generally agreed that there is more to them than that. Indeed, it is a standard feature of norm-governed organizations that particular agents (usually when acting in specific roles) are empowered to create specified kinds of states of affairs. For instance, when a priest declares a couple as married, he thereby makes it so in the eye of the church. When we speak of a policeman's power of arrest, or when we speak of a Judge's power to sentence a convinced person, we are referring to a very similar phenomenon.

It is not perhaps an oversimplification to say that there are at least two distinct senses of *right*. In the first of these, the permission to do something is combined with a prohibition to prevent the holder of the permission from doing the permitted thing. So I have a right if others have obligation not to interfere with my behaviour. In the second sense, I have a right if others (it is not always clear who) have obligations positively to see to it that I can do or have that to which I have the right.

The study of these notions of power and right is left for future work.

7 Relation to Risk Analysis Conceptual Model

Figure 10 shows part of the CORAS risk analysis conceptual model[9]. This sub-model defines the context of a risk analysis. The context consists of the stakeholders and assets of the system under analysis, which all further analysis is based on.

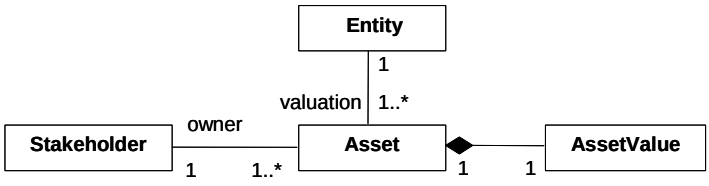

Figure 10: Risk analysis context sub-model

A risk analysis is *asset-driven*, which means that the analysis is carried out relative to the identified assets. In the general case, an asset may be anything that stakeholders of the target of evaluation find to have value.

Each asset may only be related to one stakeholder and should have an unambiguous value assigned by that stakeholder. If two stakeholders view the same entity as an asset, this should be documented as two different assets related to the same entity. Two assets are per definition different if valued by different stakeholders, as both the values they assign and the reasons for the assignment may be different.

Below the concepts of the CORAS risk analysis model are described:

- *Stakeholder*. A person or organisation that has interests in the target of evaluation.
- *Asset.* A part or feature of the target of evaluation that has value for one of the stakeholders.
- *Entity.* A physical or abstract part or feature of the target of evaluation that becomes an asset when assigned value by a stakeholder.
- *AssetValue.* The value assigned to an asset by a stakeholder.

Figure 11 shows how the concepts related to circumstance, as described in section 4, are related to various concepts from the CORAS risk analysis conceptual model. On the left hand side are the concepts related to circumstance, and on the right hand side are the concepts from the CORAS model. A **threat scenario** is a sequence of events or activities which may lead to a reduction of the value of an asset. A threat scenario is initiated by a **threat agent**, e.g. a disloyal employee or a computer virus. An actor may act as a threat agent in different circumstances.

[9] Lund, M.S., Hogganvik, I., Seehusen, F. and Stølen, K., UML profile for security assessment, SINTEF technical report STF40 A03066, December 2003.

Entity and asset are related in the CORAS conceptual model, as shown in Figure 10.

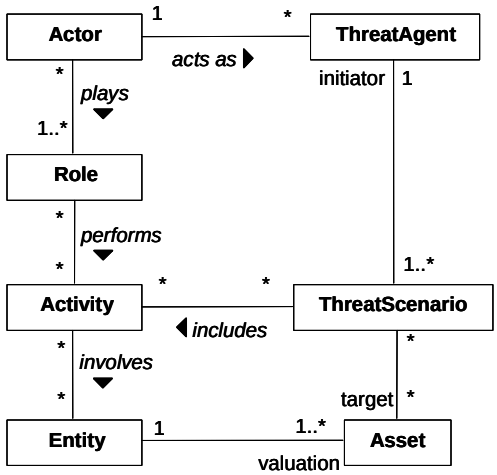

Figure 11: Integration with risk analysis conceptual model

8 Incorporating Trust, Reputation, Information and Ownership

Comment [fvr2]: What to do about "informs about"?

The client of a risk analysis may not be interested in trust as such, but rather in assets such as market share and income. **Trust** and **reputation**, however, are clearly important factors that affect customers' behaviour, and may therefore be viewed as assets of their own[10]. As mentioned in section 7, an entity is a physical or abstract part or feature of the target that becomes an asset when assigned value by a stakeholder. We therefore also view trust and reputation as subtypes of entities. Of particular interest in the context of legal risk analysis of data protection issues and intellectual property rights (IPR) are **information** assets, as well as the notion of **ownership**.

Studies of trust distinguish between the trustor, that is, the agent that trusts another agent, and the trustee; the agent being trusted. Trust can be modelled as a binary relationship from the trustor to the trustee, denoted as **source** and **target** of the trust, respectively. Ownership is modelled as a relationship between an actor, the owner, and an entity. These concepts and relationships are shown in Figure 12. The actor also plays the role of stakeholder with regards to an asset. This is the same as the stakeholder shown in Figure 10. Furthermore, actor is itself a specialisation of entity. An actor may be a natural person, i.e. a human being, or a juristic person, e.g. an organization, as well as other types of behavioral entities, e.g. a software agent.

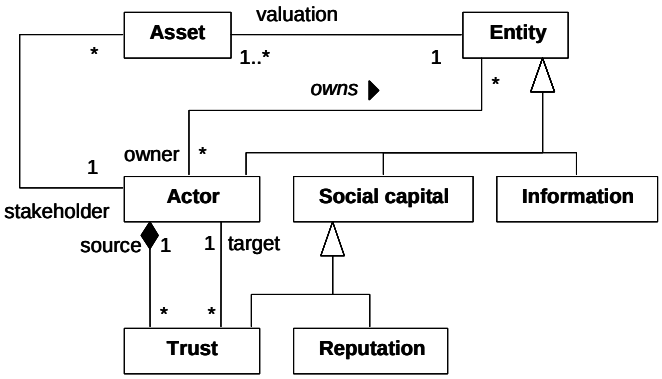

Figure 12: Refinement of entity

[10] Brændeland, G. and Stølen, K., Using Risk Analysis to Assess User Trust – A Net-Bank Scenario, Proceedings of 2nd International Conference on Trust Management, LNCS Springer, Oxford, UK, 2004.

9 Combined Model

Figure 13 shows all the concepts and models discussed in the sections above combined into a single model.

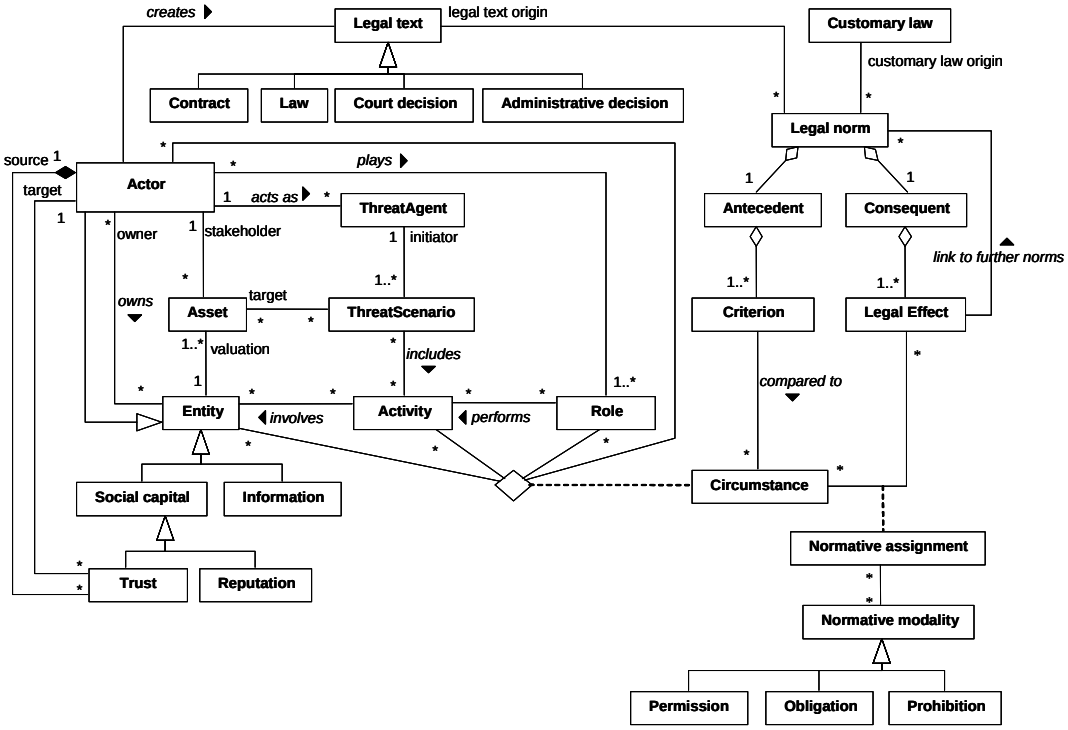

Figure 13: Combined conceptual model