SINTEF REPORT

SINTEF

SINTEF ICT

Address: NO-7465 Trondheim,
NORWAY
Location: Forskningsveien 1
Telephone: +47 22 06 73 00
Fax: +47 22 06 73 50

Enterprise No.: NO 948 007 029 MVA

TITLE

ENFORCE Conceptual Framework

AUTHOR(S)

Tom Lysemose, Tobias Mahler, Bjørnar Solhaug, Jon Bing, Dag Elgesem and Ketil Stølen

CLIENT(S)

REPORT NO. A1209	CLASSIFICATION Open	CLIENTS REF.	
CLASS. THIS PAGE Open	ISBN 978-82-14-04050-0	PROJECT NO. 90B22000	NO. OF PAGES/APPENDICES 56
ELECTRONIC FILE CODE EnforceConceptualFramework.doc		PROJECT MANAGER (NAME, SIGN.) Ketil Stølen Ketil Stølen	CHECKED BY (NAME, SIGN.) Atle Refsdal Atle Refsdal
FILE CODE	DATE 2007-03-08	APPROVED BY (NAME, POSITION, SIGN.) Bjørn Skjellaug	

ABSTRACT

ENFORCE is a multi-disciplinary research project addressing trust management. The research objectives include the development of a methodology for the capture and analysis of policies for security and trust management, the development of a methodology for legal risk analysis to ensure trust, as well as the development of a language suitable for the specification of trust management policies. This report documents the ENFORCE conceptual framework for trust management by clarifying the notion of trust and related notions, and by defining the relations between them.

KEYWORDS	ENGLISH	NORWEGIAN
GROUP 1	Trust	Tillit
GROUP 2	Risk	Risiko
SELECTED BY AUTHOR	Prospect	Mulighet, utsikt
	Security	Sikkerhet
	Legal	Juridisk

TABLE OF CONTENTS

1 Introduction

ENFORCE is a multi-disciplinary research project addressing trust management. The research objectives include the development of a methodology for the capture and analysis of policies for security and trust management, the development of a methodology for legal risk analysis to ensure trust, as well as the development of a language suitable for the specification of trust management policies. This report documents the ENFORCE conceptual framework for trust management by clarifying the notion of trust and related notions, and by defining the relations between them.

There are basically two sides to the activity or process of trust management. From the perspective of the trusting party, trust management typically involves the assessment of the trustworthiness of another party and the decision making on the basis of these assessments. From the perspective of the trusted party, trust management typically addresses the issue of increasing or correctly representing its trustworthiness.

ENFORCE will focus on trust management that is applicable at an organizational level, be it a business enterprise or any other organization. The relations of particular interest are business to business and business to customer relations in an ICT context, and how access rights, security obligations, contractual issues and other legal aspects should be managed. Trust management should be a unified process that also captures the role of social, ethical and legal norms.

In addition to consider trust relations involving humans and organizations, ENFORCE will operate with a notion of trust allowing machines to be categorized as trusting entities. This means that we will define trust as a relation that permits a machine to do assessments of and make decisions about trust.

The willingness of one party (the *trustor*) to trust another party (the *trustee*) is inevitably tied up with the trustor's willingness to accept a certain level of *risk*. This risk acceptance may be justified by the prospect of a future reward that will counterbalance this risk.

The trustor's risk acceptance embodied in a trust relationship will partly be related to the trustor's intentions. A risk analysis is conducted for the purpose of identifying the risks that may reduce the values of the stakeholder's assets. Measures should then be taken in order to remove the unacceptable risks such that potential asset value reductions are less severe or less likely to occur. Incorporating trust into this picture calls for the analysis of goals related to the identified risks. Goals may in terms of assets be defined as the objective of increasing asset values. A typical example is the risk assessment a gambler is doing. His goal is to make money in a context in which the risk is very high. This risk may be accepted when the possible gain is extremely high.

There may be many reasons for one party to trust another party. ENFORCE will investigate trust relationships that are based upon *norms*. Basically, norms are statements about the duties and obligations that given parties should comply with in given situations. The notion of norm will be related to the notion of *role*; a given norm will be applicable for a set roles and a set of contexts. When, for example, a person reaches a certain age, she or he will no longer be minor, but rather an adult. This change of role involves losing a number of rights and obligations and being given a number of new ones.

There are a number of different sources of norms. ENFORCE is in particular interested in legal, social and ethical norms. A legal norm can e.g. be stated in a clause of a binding contract between two parties. One contract partner may then trust the other for fulfilling his obligations as stated in the contract. Social norms are based upon the society's expectations about how individuals, institutions, organizations, etc. should behave in the society. These norms are related to the social roles and the society's institutional framework. Ethical norms are general and independent of the social roles and institutions.

The notion of *information security* is of key relevance to the research in the ENFORCE project. By security[17], we mean the preservation of confidentiality, integrity and availability. Generally, we may classify information that must be secured as *sensitive information.* A stakeholder for whom information has a value will have obvious incentives for protecting this information. The notion of security is, however, also tightly interwoven with legal notions such as data protection, privacy and confidential information such as trade secrets. Legal norms express obligations with respect to how personal information is to be handled or otherwise processed. The possibility of legal sanctions for unlawful processing of personal information may be an incentive for an organization to ensure law compliance and a high level of security. This is also important in relation to customer trust; although consumers may consider the underlying system to be sufficiently dependable, they may not trust this system unless there is a suitable legal framework they can fall back on should anything go wrong[19].

Whereas privacy and data protection laws on the one hand call for security measures to be implemented, they may on the other hand restrict the set of measures that actually may be taken. For example, accountability is an important aspect of integrity, and therefore an aspect of security. However, measures to achieve accountability (and in particular, the special case of non-repudiation) may sometimes conflict with rules and regulations for data protection and privacy.

In the next section we will describe the research method we followed during our work on establishing the ENFORCE conceptual framework, and how it was validated. The section will furthermore explain our strategies for documenting and presenting the concepts introduced in this report. Section 3 introduces a set of central concepts on which the notions introduced in subsequent sections are based. In Section 4 the notion of risk and its dual, prospect, are introduced, while we in Section 5 explain the relevance of the notion of norm to the ENFORCE project and show how norms relate to other concepts. The notion of trust will be introduced in Section 6 before we finally conclude.

2 Research Method

The introduction of a conceptual framework for trust management serves several purposes. Importantly, such a framework provides a substantial basis upon which our future research and results rest: The conceptual framework will mark out our course, in particular by clarifying what ENFORCE aims to address, what is our understanding of central notions within trust management, and also what is considered out of scope. Moreover, the fact that ENFORCE is a multi-disciplinary research project demands a common conceptual fundament that is agreed upon, preventing conceptual confusion and ensuring a shared basis within the project.

A natural and important additional aim of establishing a conceptual framework is to clarify the relationship between the ENFORCE project and state of the art within trust management research. Our basic approach is to build the ENFORCE conceptual framework upon established state of the art concepts, while doing accommodations and adjustments where seen necessary or appropriate. There are foremost two reasons for doing adjustments of already established notions. On the one hand there may be a need to adjust the precise meaning of existing notions for the purpose making notions from different sources fit into our unified framework. On the other hand we occasionally see the need to adapt the definition of existing notions, not necessarily because we oppose to the current meaning, but rather because ENFORCE emphasizes other aspects or properties than those stressed in the source.

To the extent that we define notions in accordance with established use and established definitions we ensure that there are major research communities sharing our understanding and use. There are, however, cases in which we differ somewhat from existing definitions. An important objective is to carefully choose a terminology that harmonizes with the everyday use of this terminology in English prose. This will facilitate common understanding and prevent conceptual confusion.

We will in our conceptual clarification focus particularly on risk, risk being a notion strongly related to trust. Our primary source for the capture of the notion of risk and related notions is the CORAS[2][14] conceptual framework for security risk analysis. The CORAS conceptual framework builds strongly on standards such as ISO/IEC 17799[17] on information security, the AS/NZS 4360[1] standard on risk management and the ISO/IEC13335 guidelines for management of IT security. Since CORAS builds on standardized terminology we ensure that our ENFORCE notions will be defined in a way that is closely related to accepted terminology by using CORAS as a source. The CORAS terminology has furthermore been thoroughly tried over several years both through research and publications, and by being deployed and tested empirically in several security risk analyses of various larger information systems.

Since CORAS is particularly directed towards problems of information security risks, there are a number of further notions related to e.g. trust and law that are not covered there. Our strategy is to continuously consider notions and definitions as established in state of the art literature and build on them when suitable, for example the paper on the use of CORAS for the specification of legal risk scenarios [29].

There is, however, one aspect of trust that we may capture neatly by departing from our notions related to risk, viz. the aspect of prospect. Recall that just like trust is related to risk, it is also related to the possibility of a future reward. The choice to establish a trust relation with another party involves the acceptance of a certain degree of risk, but the incentive to this risk acceptance is that by relying on another party to act in a, to the trustor, benign way, the trustor may achieve things he or she could not as easily have obtained alone. Such a choice is often modelled as a rational choice within a theory of expected utility, see e.g.[30], that when applied to a trust relation basically says that one should engage in a given relation of trust in case the expected positive utility of success outweighs the expected negative utility of failure.

Our term "prospect" is taken from prospect theory as introduced by Kahneman and Tversky[21]. In this document the notion of prospect denotes the dual to the notion of risk, which differs somewhat from how it is used in prospect theory. Whereas Kahneman and Tversky's notion of prospect denotes the whole set of possible outcomes of a choice problem, both good and bad, we will refer to the positive outcomes as prospects and the negative outcomes as risks. Since the notion of prospect in our context is perfectly dual to our notion of risk we are automatically provided definitions of prospects and related notions as soon as the corresponding notions of risk are captured. This also means that the use of the CORAS terminology as a foundation for our risk related concepts is as suitable as a foundation for our notions related to prospect.

The validation of our conceptual framework will in this report be done by the continuous reference to an example in which the majority of the notions we introduce are illustrated. A substantial part of the terminology will to some extent have been extensively validated by the fact that we adopt established notions from e.g. CORAS, and further testing of the framework will be carried out through future ENFORCE activities such as case studies and publications.

The notions we introduce will be modelled in UML 2.0[27] class diagrams. They will as a rule be precisely defined in English prose, and sources or related literature will be referred to. Our formal approach to the capture of concepts of relevance to the ENFORCE project is further reflected in the examples in which other UML 2.0 diagrams, such as sequence diagrams, are deployed.

Example 1

We have chosen eBay as the context of the ongoing examples, and will in particular look at one specific transaction between two users.

Our model of eBay is given in Figure 1. There is on the one hand the auction system that controls the posting of offers at eBay and the bidding process that may lead to the winning of an auction. On the other hand there is the payment transaction system PayPal that eBay offers to its users for money transfer. PayPal communicates with the credit card companies that are responsible for the actual money transfer.

Additionally, eBay has a register of all its users as captured by the User class. Each user is identified by its e-mail address and has additionally a reputation score that is derived from the judgement of other eBay users. The users divide into two, buyers and sellers.

We will throughout this document assume two eBay users, Sally and Billy. Sally is a seller that has posted an offer on the eBay market platform. The item she wants to sell is a digital camera. We will not go into any of the details about the bidding process, only focus on Sally and the bidder, Billy, who ends up winning the bidding round and buying the camera.

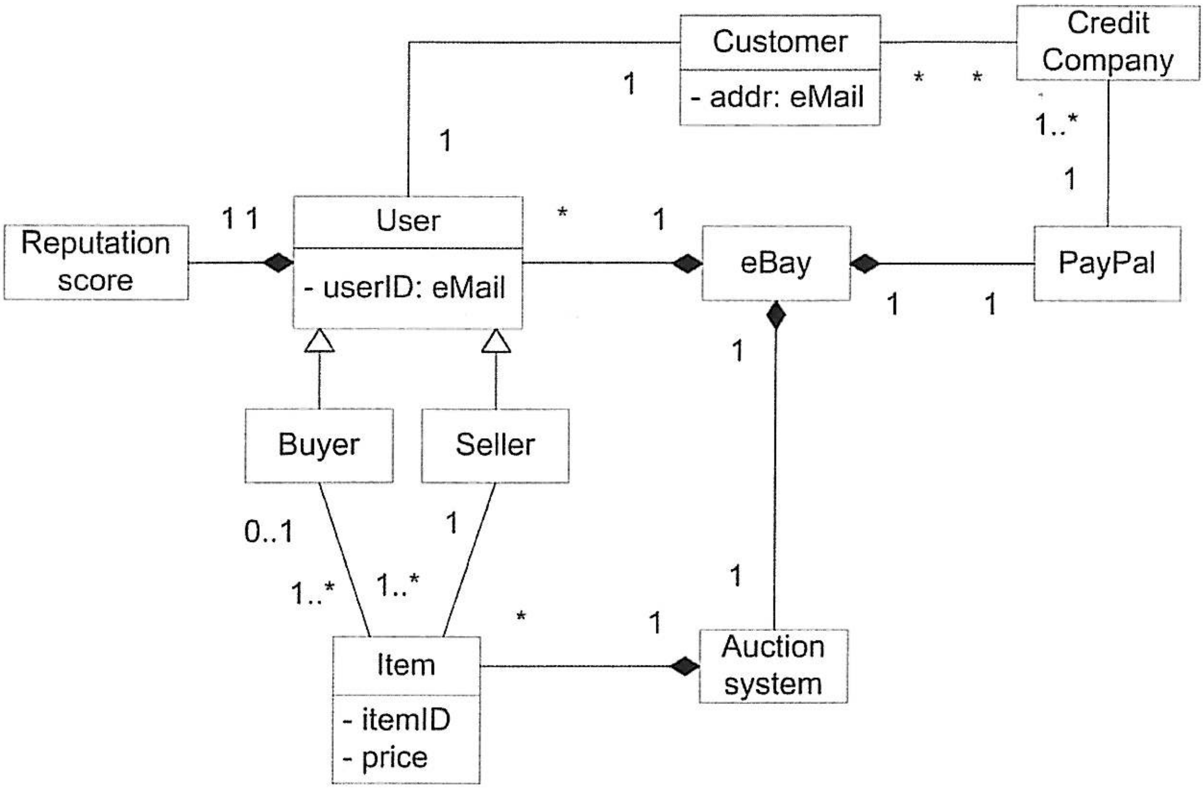

Figure 1 – eBay

The rationale for choosing eBay as an example case is threefold: First, trust issues in eBay have received a considerable amount of attention in the scientific community. The reason for the general interest in eBay may be grounded on the fact that the relation between a buyer and a seller in eBay is mediated through the Internet, and both parties neither are expected to have prior knowledge of each other, nor will meet each other in the normal course of their transaction. Given the academic interest in eBay, we may expect that the trust issues in eBay are relatively well understood. Second, eBay seems relatively well suited since the transaction between a seller and a buyer exemplifies the interplay of trust and risk and shows the how legal aspects play a role in the transaction. Third, it is considered beneficial that the case will be relatively familiar to readers, thereby facilitating them to understand how the abstract concepts in the ENFORCE conceptual model relate to a concrete and well-known real-world scenario.

3 Basic Concepts

We will in this chapter define a number of concepts on which notions introduced in succeeding chapters are based. An important aspect of most of the notions of this chapter is that they are *descriptive* in the sense that they refer to aspects of the state of affairs objectively and independent of subjects such as a stakeholder.

3.1 Entity and Actor

The term *target* is used to denote a particular set of related objects. An *entity* is a physical or abstract part or feature of the target that may be passive or active. Both passive and active entities may be acted upon.

Entity: A physical or abstract part or feature of the target. An entity is active or passive. An active entity can initiate activities or interactions, while a passive entity interacts by responding when acted upon.

Actor: An active entity which has goals, intensions and capabilities. An actor is an organization, a human or a machine.

Machine: An automated artefact such as hardware and software.

Organization: An actor having other actors as members.

The notion of entity is adopted from the CORAS[2][14] terminology, while the notions of actor and organization are based on TROPOS[3][4]. The definition of machine is closely related to the corresponding notion in the Reference Model for Open Distributed Processing[16], however here defined such that it fits with the more general notions of actor and entity. The class diagram of Figure 2 describes the notion of actor and shows how actors and organizations may be composed.

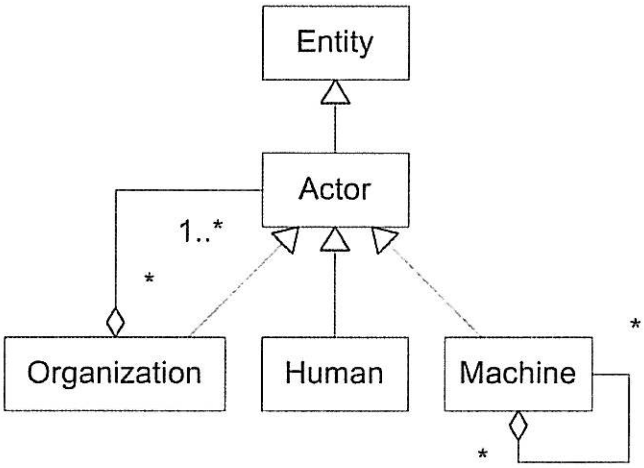

Figure 2 – Actor and Organization

Example 2

Figure 3 shows a combination of elements from the entity model of Figure 2 on the one hand and elements from the eBay class diagram of Figure 1. The items that are posted at eBay and the reputation score are the entities that are not actors, the latter being an abstract entity. A customer is either an organisation or a human. The xor constraint between the relations to the customer means that a customer cannot be both organization and human.

An instance diagram could also have been provided here in which the organizational structure of eBay would have been decomposed into the sub-organizations PayPal and AuctionSystem. Sally and Billy would be instances of Customer and User, as well as Seller and Buyer, respectively. Their specific reputation score would be instances of Reputation Score and the camera an Item instance, all of them furthermore Entity instances.

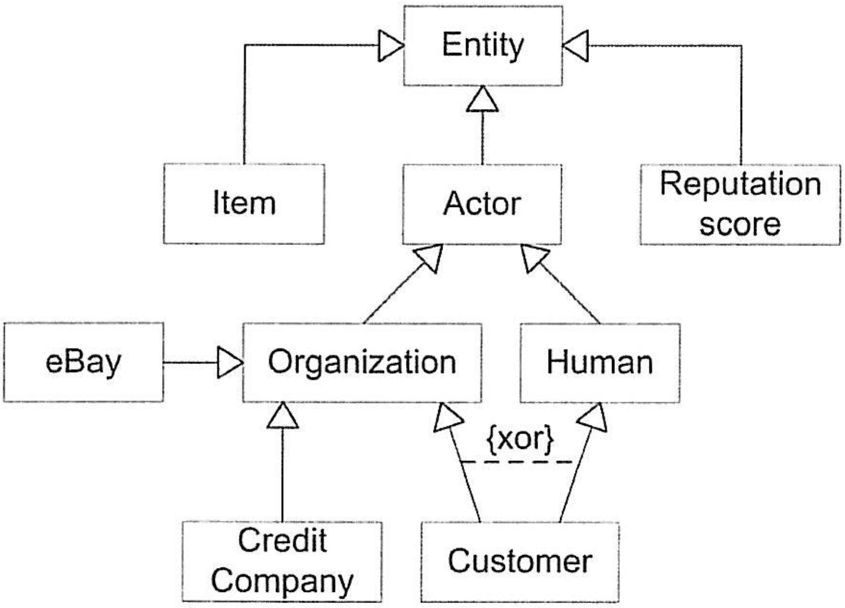

Figure 3 – eBay entities

3.2 Scenario

A scenario is understood as an interaction involving a number of entities, and the execution of a scenario corresponds to a sequence of states. The initial state of the sequence is a snapshot of the target at the moment the execution is started up. The following states describe step-by-step how the target changes. The same scenario may have several different executions.

State: A state is a snapshot of the target. The state of the target may change over time.

Scenario: A scenario is a set of *sequences of states*. It involves a number of entities some of which may perform actions and some of which may interact.

Transition: A transition is a change of state from *pre state* to *post state*. The change of state is caused by the activity of some entity in the scenario.

Likelihood: The frequency or probability for the scenario to occur. The notion of likelihood is adopted from CORAS[2][14].

Scenario relation: Scenarios may be related in different ways, e.g. composition like sequential or parallel. Scenarios may hence generally be decomposed into several sub-scenarios.

The notion of a scenario and related concepts are described in the class diagram of Figure 4.

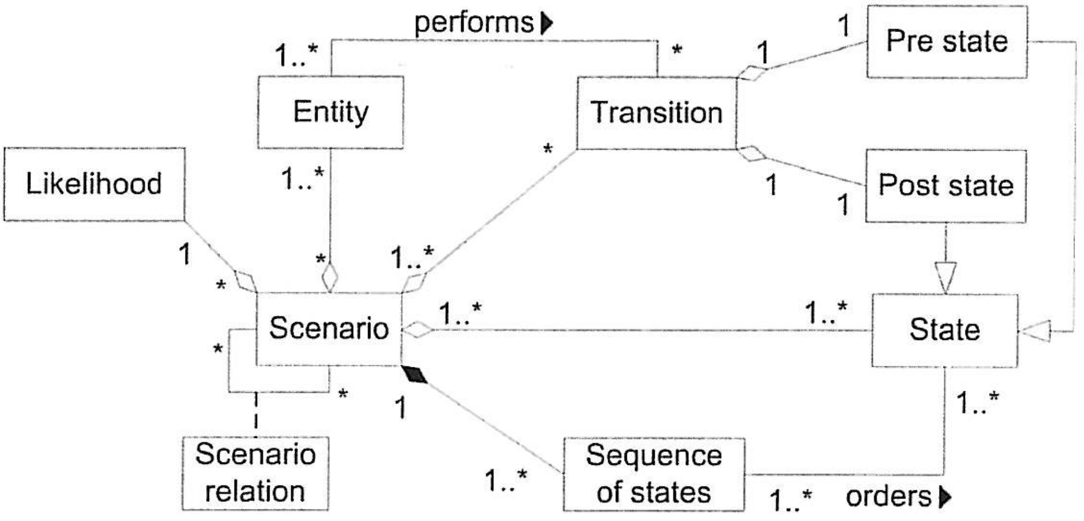

Figure 4 – Scenario

Example 3

A range of scenarios is played out during the time from Sally's posting of her offer at eBay until Billy receives the camera after having won the auction and paid for the item. Since scenarios can be composed of other scenarios, we may choose whether to describe the whole process as one or more scenarios.

A scenario may be interpreted in terms of UML 2.0 sequence diagrams as shown in Figure 5. This scenario is composed of three sub-scenarios, viz. the bidding process, the payment process and the shipment of the camera. In this case, the three scenarios are related by sequential composition.

There are four entities in this scenario represented by one lifeline for each entity. We assume that Billy and Sally are humans, whereas eBay and the credit company are organizations.

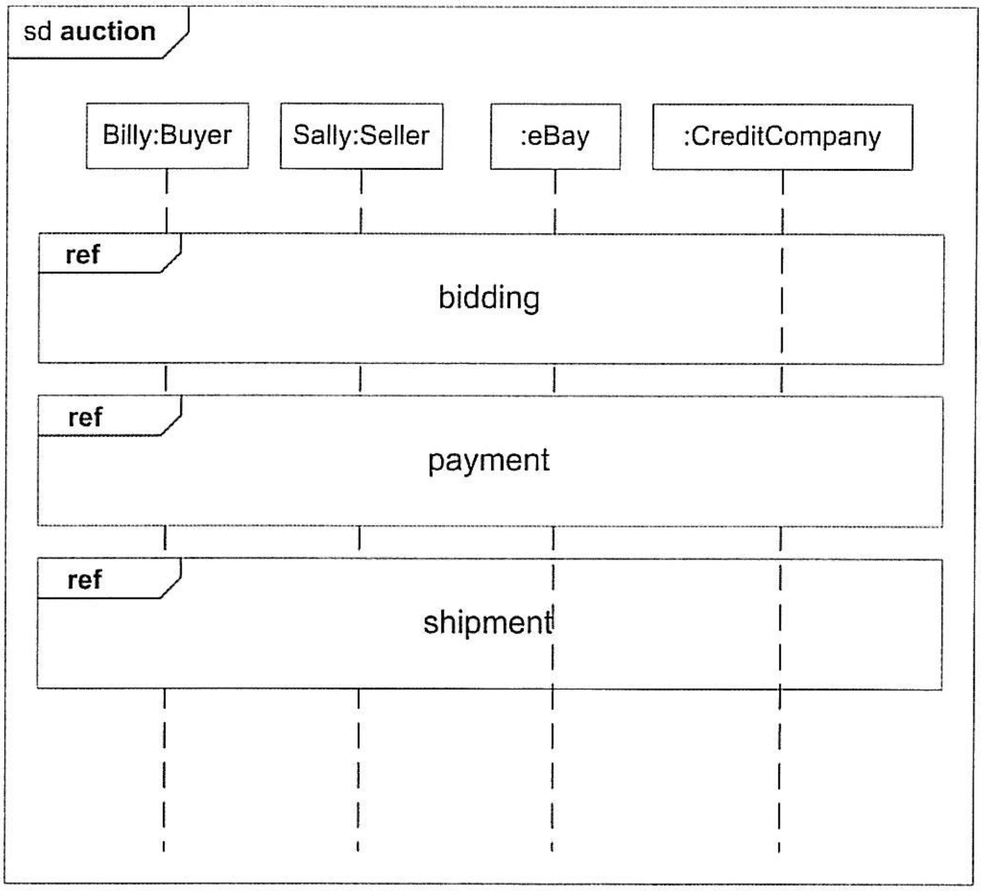

Figure 5 – eBay auction

Example 4

Figure 6 shows the sequence diagram describing the payment scenario. Each eBay user has an attribute showing the number of items that is yet to be paid for. In this scenario Billy's account in eBay initially shows *n* items to pay for and eventually *n-1*, assuming that he has not won any auctions in between.

UML 2.0 sequence diagrams allow the state of entities to be specified (local state in terms of UML). In this scenario we see that there is a change in Billy's state, and hence a change of the scenario state also (global state in terms of UML).

The global state in which *Billy.unpaidItems=n-1* that follows immediately after the global state in which *Billy.unpaidItems=n* represents a transition performed by Billy. The latter state is the pre state and the former state is the post state of this transition. Each element of the set of sequences of states in this scenario orders the pre state of this transition to appear before the post state.

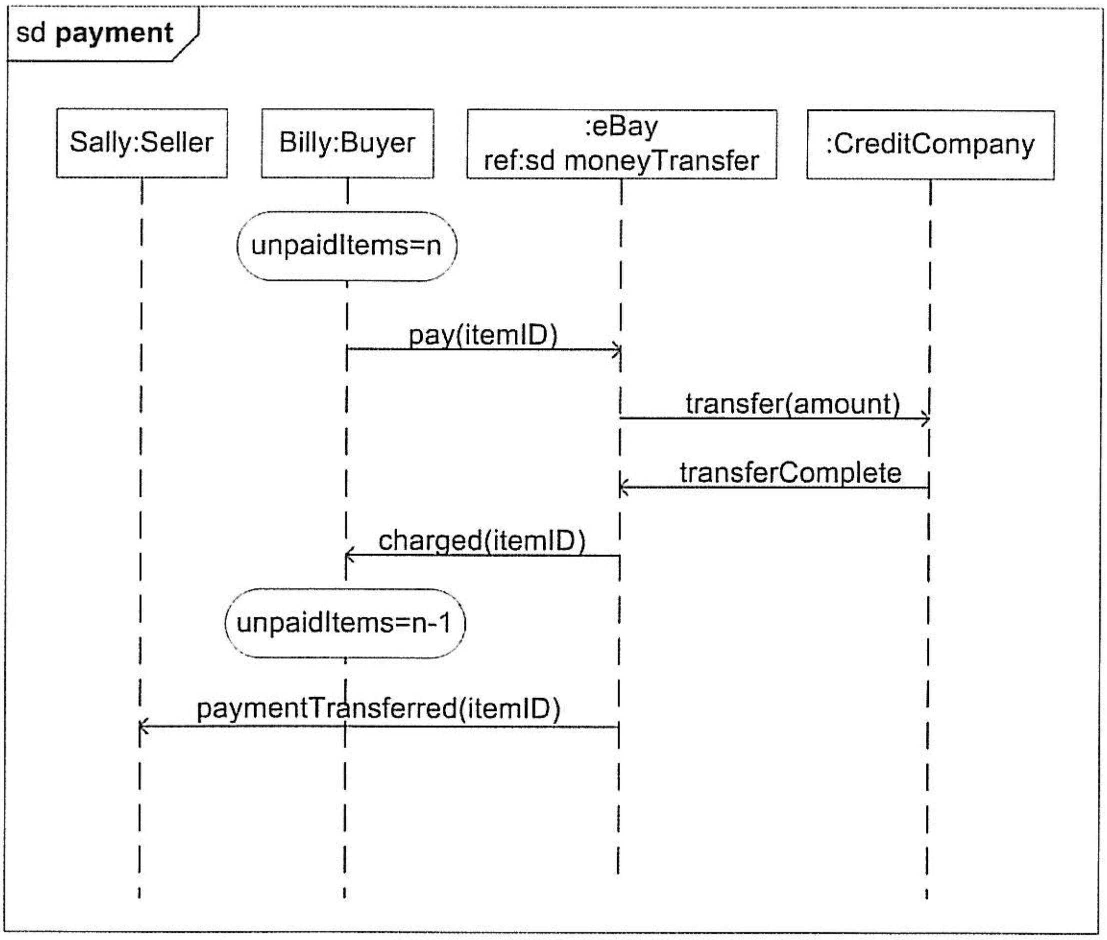

Figure 6 – Payment

Example 5

Figure 7 illustrates how lifelines may be decomposed into several lifelines. In this case the :eBay lifeline of Figure 6 is decomposed into the two lifelines :Auction System and :PayPal. This kind of decomposition is reflected in the conceptual model in that organizations may have actors, including sub-organizations as members.

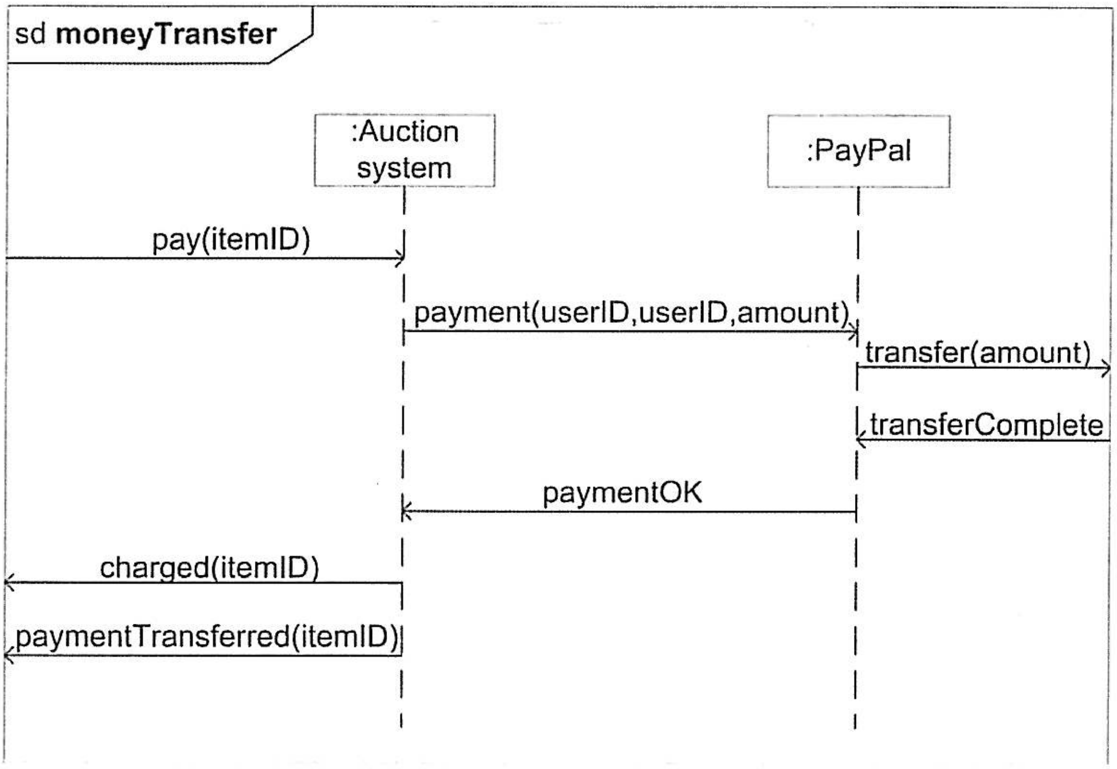

Figure 7 – Money Transfer

3.3 Asset

The notion of asset is directly adopted from CORAS[2][14] and defined as follows:

Asset: An asset represents an entity to which an actor, the *stakeholder*, directly assigns value.

Asset value: The value of an asset in terms of its importance to the stakeholder.

The actor to which an entity has some value is referred to as a stakeholder. Notice that an entity may be an asset for more than one stakeholder and that the asset value is a subjective value assigned by the stakeholder. The same entity may hence be assigned different values by different stakeholders.

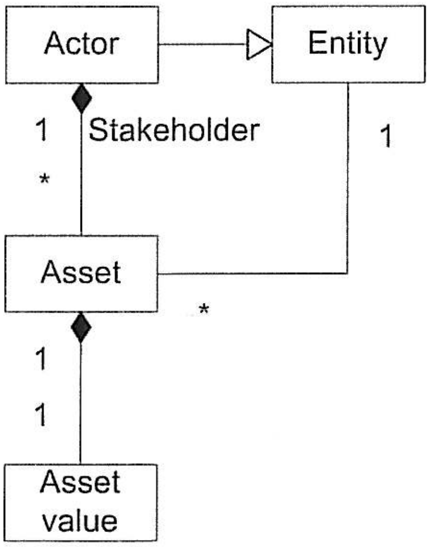

Figure 8 – Asset

3.4 Role

Role: A role is an abstraction of a number of actors, for example employee, student or customer. A role is modelled as an aspect of an actor.

The concept of role is captured by the class diagram of Figure 9. Our depiction of this notion in a class diagram differs slightly from the corresponding class diagram in[29], although the understanding and textual definitions are corresponding. Notice that an actor must have at least one role and that there may be roles that are currently not possessed. A role may furthermore be played by several actors.

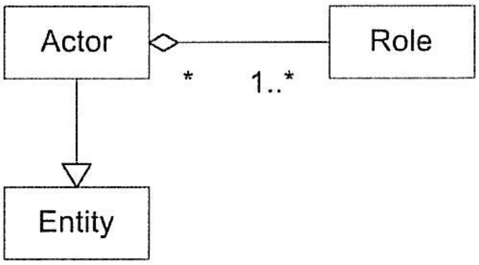

Figure 9 – Role

Example 6

Figure 10 illustrates an eBay payment more generally than the sequence diagram of Figure 6 by not specifying who instantiates the buyer and seller roles. The buyer and seller are here any eBay users. As roles may change over time and as an actor may have several roles, Billy may for example act as a seller in another scenario.

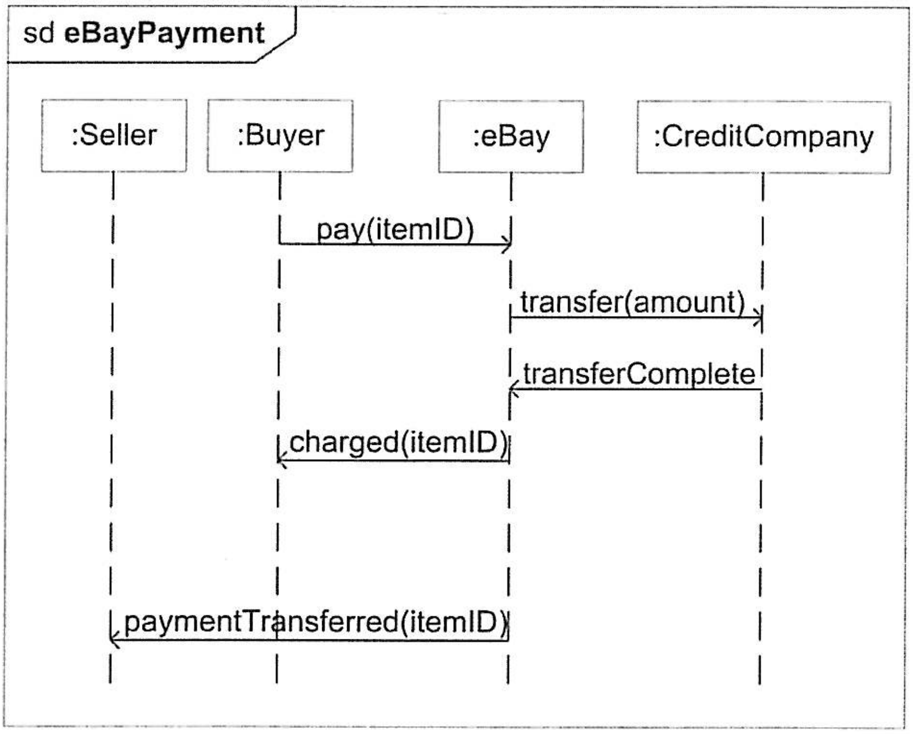

Figure 10 – Roles

4 Risk and Prospect

This chapter introduces a number of concepts that are derived from the notions of the previous chapter. Whereas most of the above notions are of an objective character, the concepts of this chapter are generally of a subjective character.

Notice, importantly, that it is the notion of asset that introduces the subjective aspect: One and the same entity may be an asset to one party but of no value to another.

4.1 Risk

In this sub-section we define the notion of *risk*, while the next sub-section covers the dual notion of *prospect*. Basically, all notions introduced in this section are directly adopted from CORAS[2][14], which in turn are based on several established standards[1][12][15][17].

Incident scenario: An incident scenario is a scenario that (if it occurs) will reduce the value of at least one asset.

Risk: A risk is the chance of the occurrence of an incident scenario. The risk value is measured in terms of consequence (decrease of asset value) and likelihood.

The subjective aspect of a risk stems from the consequence part: Just like the assignment of value to an asset depends on the stakeholder, so does the consequence value.

The class diagram for the concept of risk is given in Figure 11. Notice that a risk is inevitably tied up with an asset, and hence also a stakeholder, for without an asset there can be no risk.

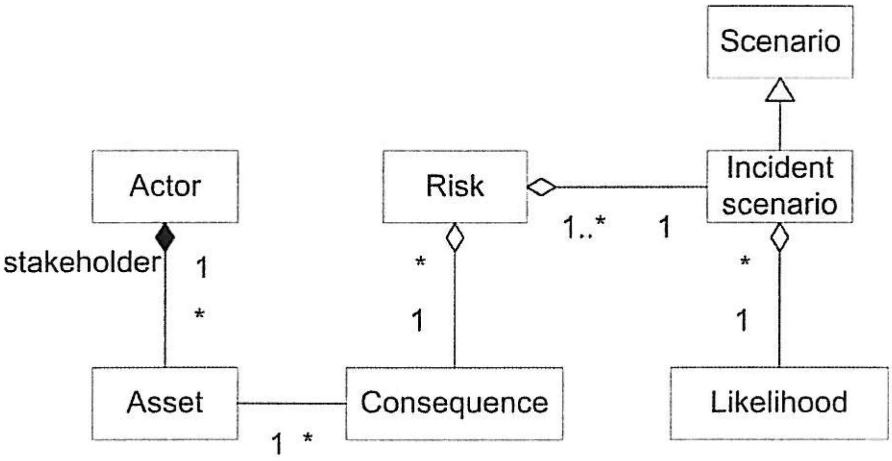

Figure 11 – Risk

4.2 Prospect

As will be clear from the definitions, the notion of prospect is the dual to the notion of risk. CORAS[2][14] does not operate with the concept of prospect, but since it is defined as the dual to risk, we may refer to CORAS as the source to this notion also. The same holds for a number of the notions introduced below.

Opportunity scenario: An opportunity scenario is a scenario that (if it occurs) will increase the value of at least one asset.

Prospect: A prospect is the chance of the occurrence of an opportunity scenario. The prospect value is measured in terms of consequence (increase of asset value) and likelihood.

Figure 12 gives the class diagram for the notion of prospect.

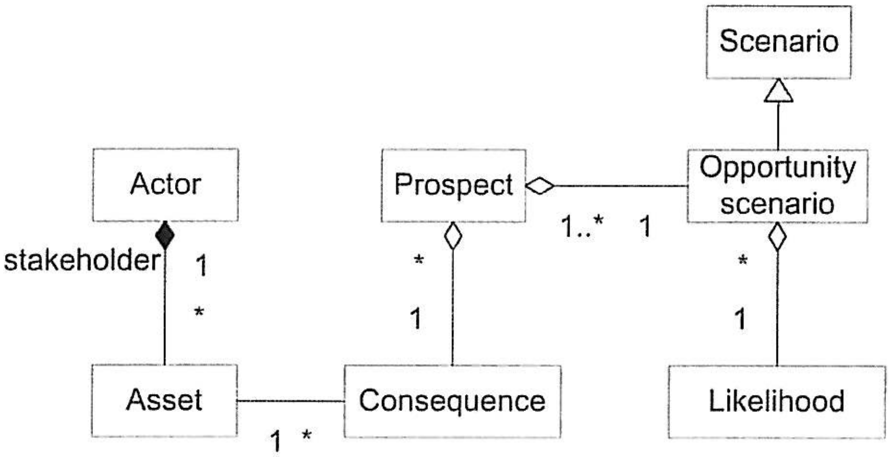

Figure 12 – Prospect

Notice that a scenario may simultaneously represent both a risk and a prospect with respect to one and the same stakeholder. A scenario may hence be both an opportunity scenario and an incident scenario.

Example 7

All the sequence diagrams given above are objective in the sense that they describe scenarios independent of who are the stakeholders, what are the assets, what are the threats, etc. To get a complete description of risk and prospect scenarios, they must be modelled from the viewpoint of a particular stakeholder: For a given stakeholder we identify assets, asset values and consequence values.

In Figure 13 we show how aspects of risks and prospects can be captured by state descriptions in an objective interpretation of the composite auction scenario. Assume that Billy won the auction by placing the highest bid of €50. Assume further that Billy holds the camera to be worth €60 and that Sally values the camera to €40. This trade is hence beneficial for them both. We see from the diagram that the scenario that is given by the sequential composition of the bidding and payment scenarios is a risk for Billy and a prospect for Sally: Billy's savings are reduced with €50 whereas Sally's savings are increased with the same amount. The shipment scenario on the other hand is a prospect for Billy. The auction scenario hence involves both risks and prospects. The aggregated asset values are, however, greater at the post state of the auction scenario than the aggregated asset values at the pre state for both the actors.

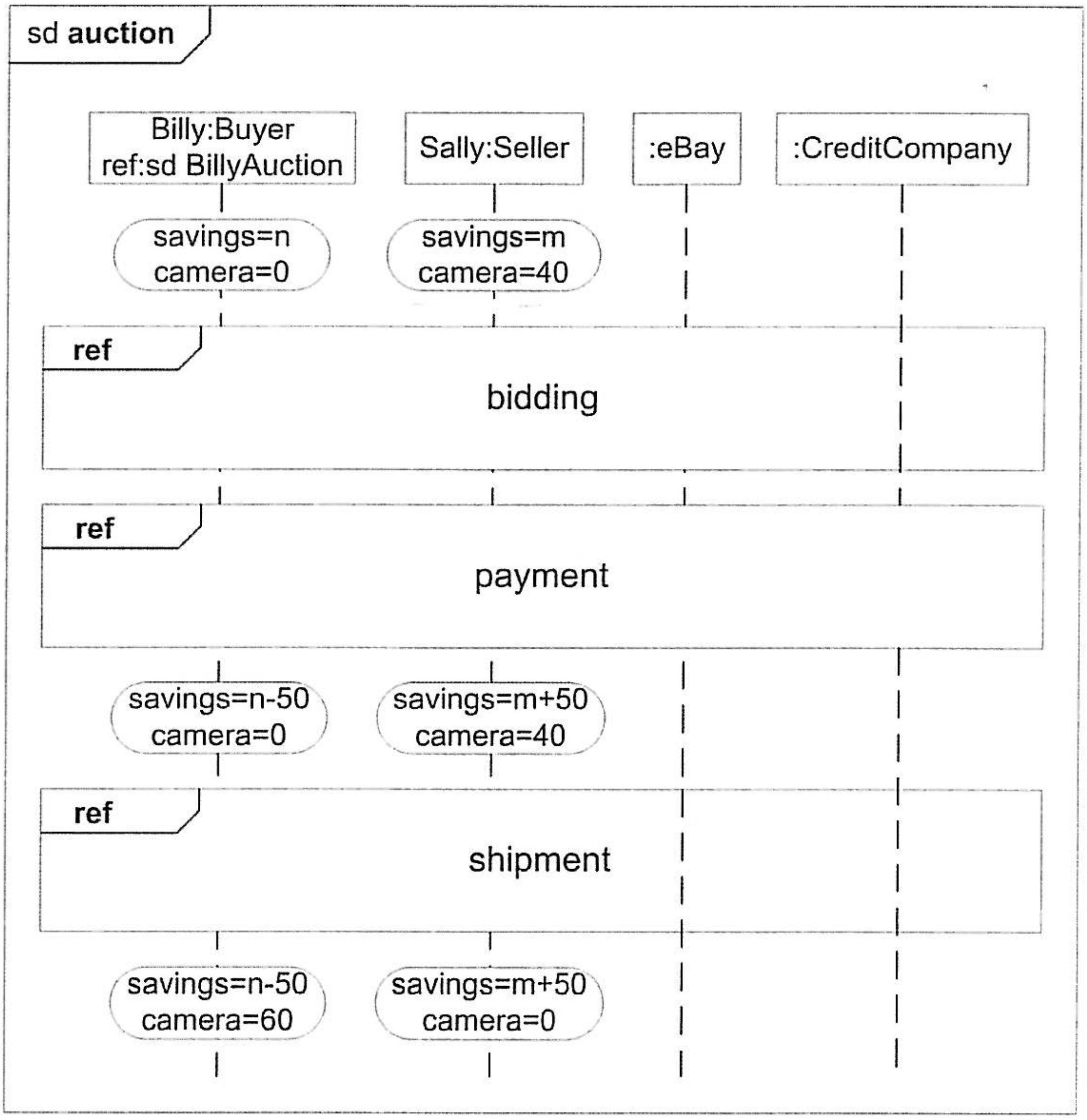

Figure 13 – Risk and prospect objectively

Example 8

A more complete modelling of risks and prospects is given by the capturing of asset, asset values and consequence values with respect to a given stakeholder. In Figure 14 the eBay scenarios of payment and shipment is described from Billy's point of view. Notice that the interactions of bidding, payment and shipment involve transactions with the actors shown in Figure 13, although not explicitly shown in Figure 14.

Recall that an asset is an actor's subjective assignment of a value to a physical or abstract entity. An asset can hence be seen as an attribute of an actor with a reference to some entity. In this sense we may view the three lifelines of the sequence diagram of Figure 14 as being a decomposition of the Billy lifeline in the above sequence diagrams. The assets cannot exist without the existence of the stakeholder.

A sequence diagram describing some other stakeholder, e.g. Sally, may have assets referring to the same entities, e.g. the camera. Importantly, an asset lifeline for one stakeholder must never be confused with the asset lifeline for another stakeholder, although they refer to the same entity.

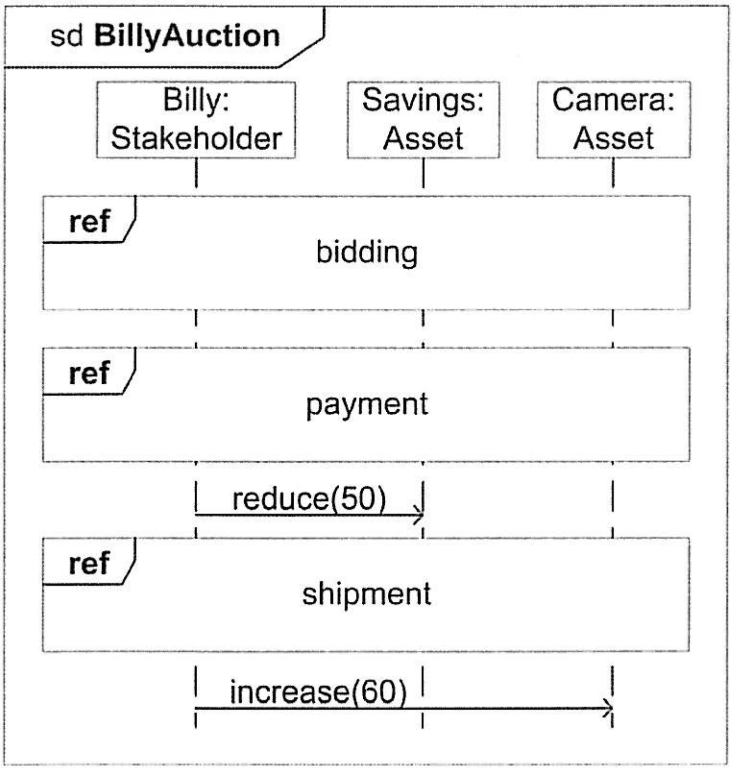

Figure 14 – Risk and prospect subjectively

4.3 Vulnerability

Vulnerability: A weakness, flaw or deficiency that opens for a *threat* to reduce the value of one or more assets.

The class diagram capturing the notion of vulnerability is given in Figure 15. A threat is defined as a role which may be played by an actor. A threat is like an asset or an incident scenario a subjective notion, i.e. a role that is assigned to an actor by a stakeholder.

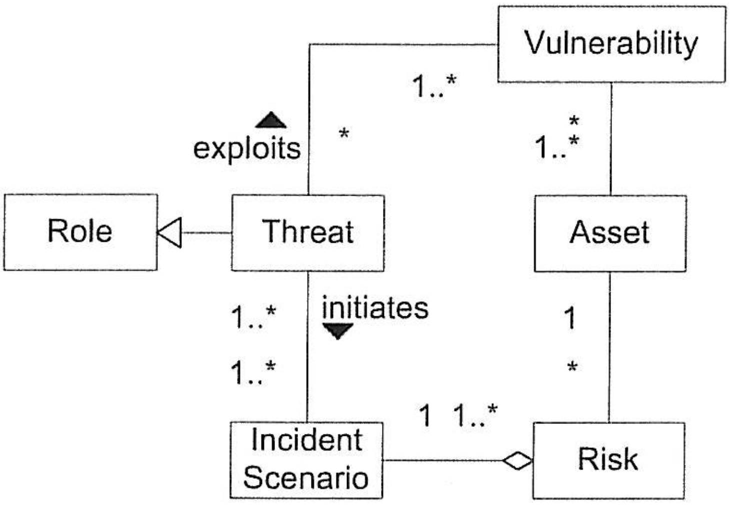

Figure 15 – Vulnerability

4.4 Strength

Strength is the dual to the concept of vulnerability and is hence an aspect that may have a positive effect on values.

Strength: An advantage, quality or potential that opens for a *facilitator* to increase the value of one or more assets.

Figure 16 gives the class diagram for the concept of strength. Notice that the role of a facilitator is defined as the dual notion to a threat.

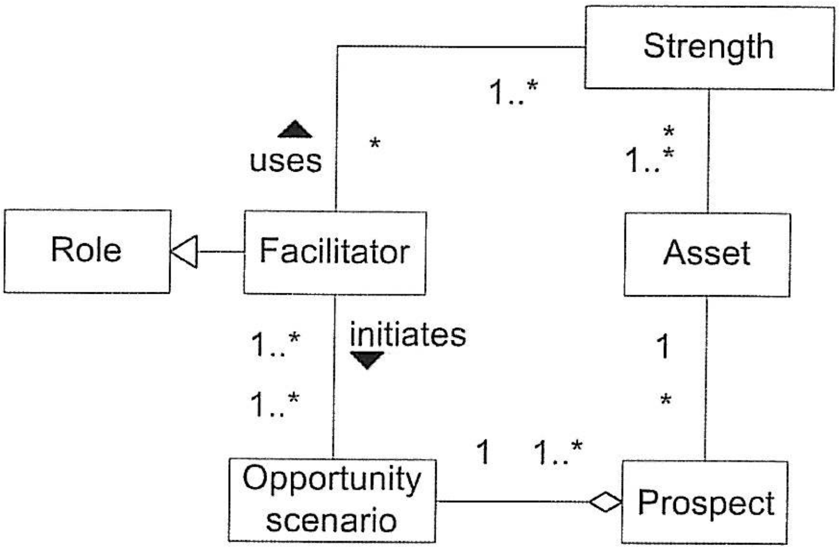

Figure 16 – Strength

Example 9

A vulnerability is a potential property of the target that may be expressed as a proposition that evaluates to true or false. If the proposition evaluates to true, the weakness is present to some degree. In terms of sequence diagrams a weakness can be specified as a condition, a guard, on an alt operand. If the guard evaluates to true the operand executes. The case for a strength is symmetrical.

Figure 17 shows the different alternatives for an exchange of payment and the item of sale. The first operand captures the current eBay practice of transferring the money before the item is shipped. This alternative represents a weakness from the viewpoint of the buyer as it opens for the seller, in the role of a threat, to keep the payment without shipping the camera in return.

The second operand shows the situation in which the item is shipped before the transaction of the payment. Such a practice represents a strength for the buyer. It may initiate an opportunity scenario in which the seller is the facilitator.

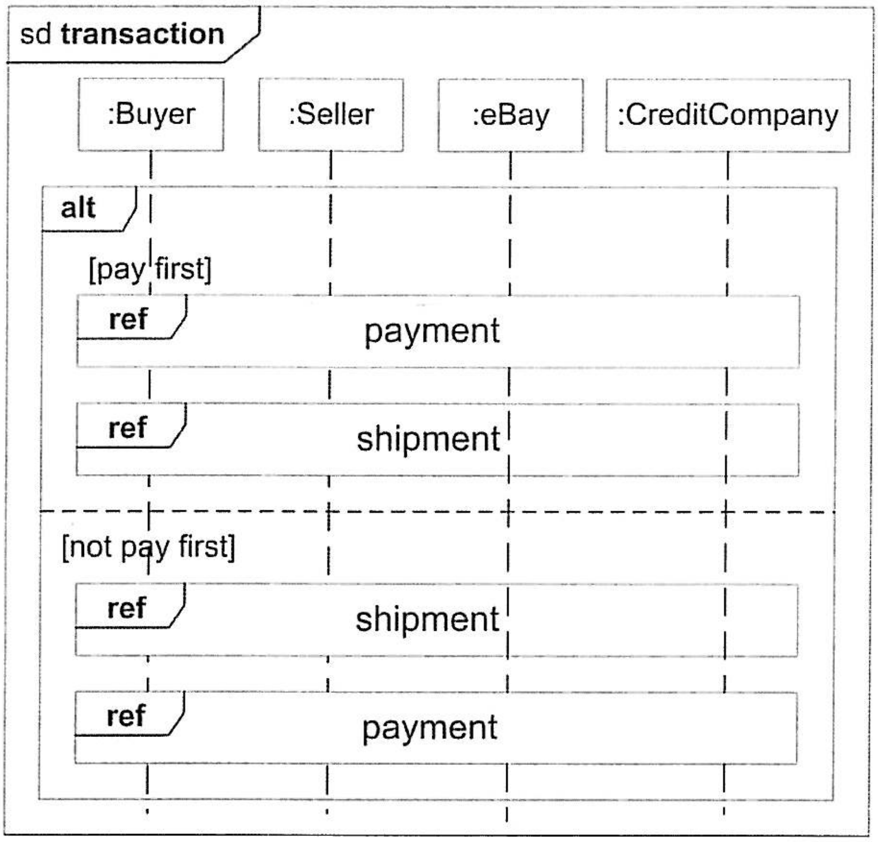

Figure 17 – Strength and vulnerability

4.5 Treatment

Treatment: A treatment is a means that is directed towards one or more risks with the objective of reducing their risk values.

Risk reduction is achieved by reducing the likelihood and/or the consequence of an incident scenario. Figure 18 gives the class diagram for the notion of a treatment.

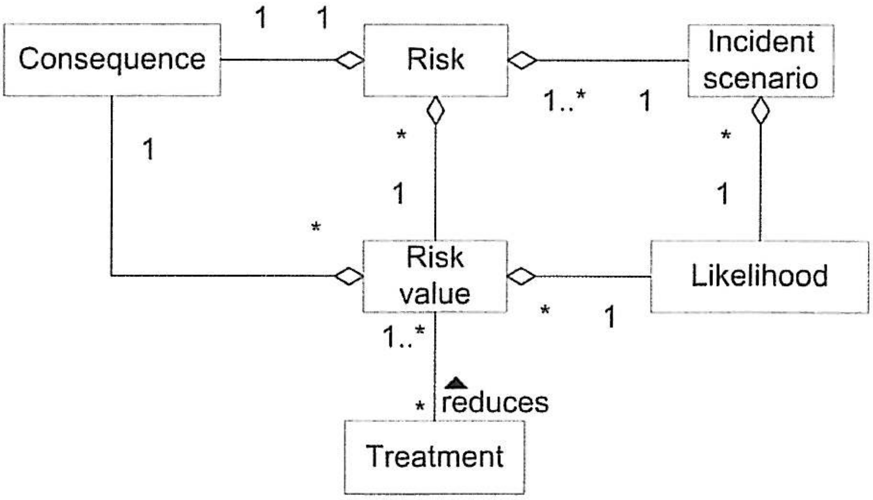

Figure 18 – Treatment

4.6 Improvement

Improvement: An improvement is a means that is directed towards one or more prospects with the objective of increasing their prospect values.

Opportunity increase is achieved by increasing the likelihood and/or the consequence of an incident scenario. This dual to the notion of treatment is modelled by the class diagram of Figure 19.

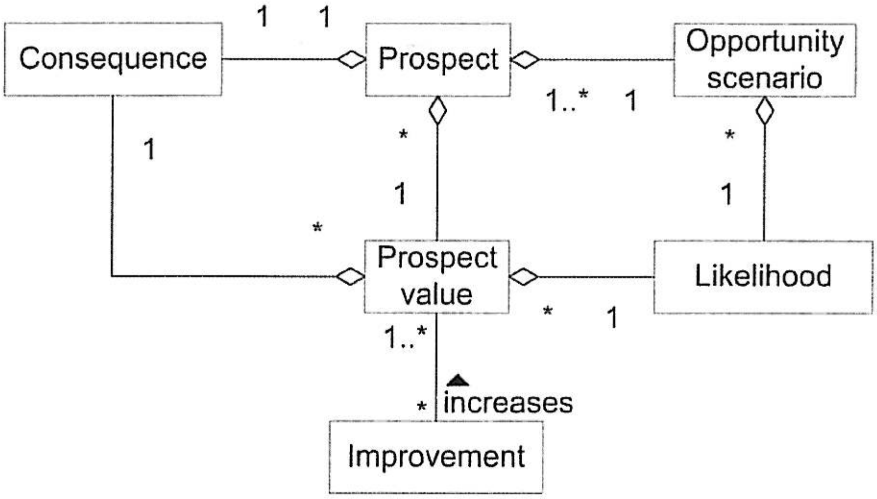

Figure 19 – Improvement

5 Rule: Regularity and Norm

This section addresses rules, including legal and other norms as well as the more descriptive regularities. This section aims thus to distinguish between factual and a normative perspective, building on Kant's[22] distinction between "the *is*" and "the *ought*".

5.1 Rule

Rule: A rule is defined as a relation between two particular scenarios, an antecedent scenario and a consequent scenario.

Modality: The modality is a statement about *how* the two scenarios are related. The relation between the two scenarios depends on the type of rule, as will be discussed in the following sections.

The class diagram for the notion of rule is given in Figure 20.

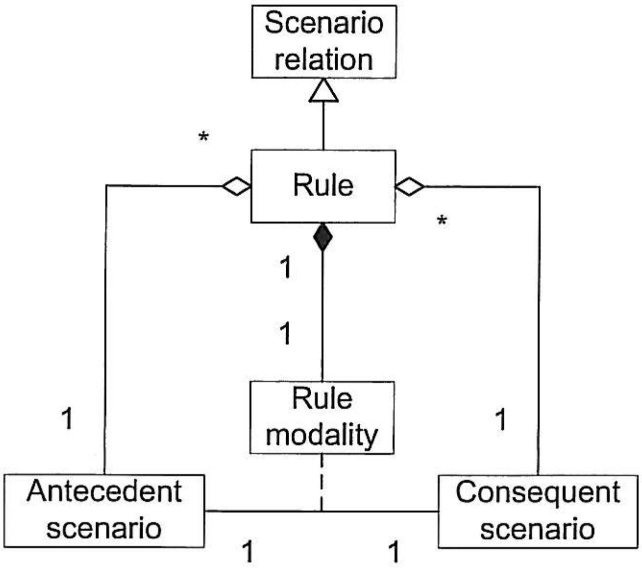

Figure 20 – Rule

Examples of rules will be given in the following sub-sections, which address certain types of rules, namely regularities and norms.

5.2 Regularity

Regularity: This is a rule of a descriptive type, relating an antecedent scenario and a consequent scenario. The regularity indicates that, given the antecedent scenario, the consequent scenario will regularly occur.

Regularity modality: A regularity modality is a statement about how the regularity relates the two scenarios. Examples of regularity modality include causality (according to observable laws of nature) as well as human or machine decision.

The class diagram for the notion of regularity is given in Figure 21, and examples of regularities in the eBay example are provided in Example 10 and Example 11.

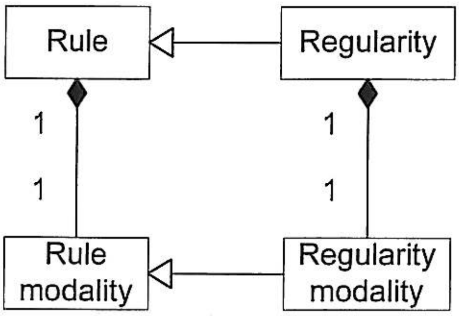

Figure 21 – Regularity

Example 10

In the eBay example, buyers and sellers can register comments in the feedback forum, in order to make these available to other users. *Regularly*, eBay publishes these comments on its web sites, as illustrated in Figure 22.

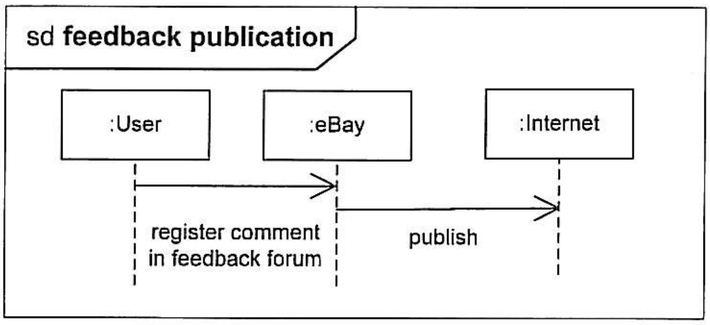

Figure 22 – Regularity in eBay feedback forum

Example 11

In practice, there may be some kind of human or machine decision. eBay may for example ensure that the language utilized in the feedback forum is adequate for publication, and the decision for publication may depend on the result of a language check as illustrated in Figure 23, possibly performed by a machine.

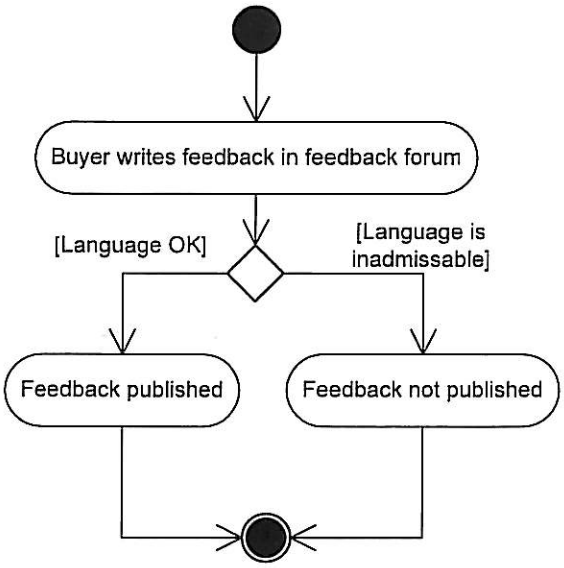
Buyer writes feedback in feedback forum
[Language OK]
[Language is inadmissable]
Feedback published
Feedback not published

Figure 23 – Regularity in decision by eBay feedback forum

5.3 Norm

In this section we introduce the concept of norm, which will be relevant for the understanding of legal aspects as well as trust and policies. The concept of norm presented here is particularly influenced by legal theory and modal logic.

Norm: A norm is a type of rule, relating an antecedent scenario and a consequent scenario. The norm indicates that, given the antecedent scenario, the consequent scenario *ought to be* or *ought not to be.*

The class diagram for norm is given in Figure 24.

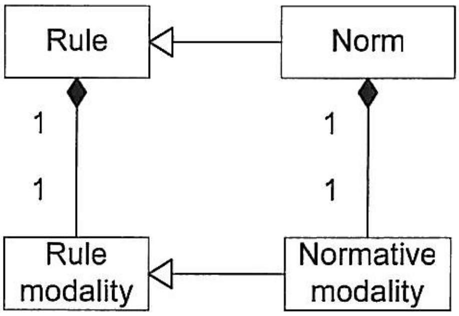

Figure 24 – Norm

Normative modality: The normative modality is a statement about how the two scenarios are related, i.e. it describes the normative status of the consequent scenario, given the antecedent scenario.

Figure 25 illustrates that the regularity modality and normative modality are specific types of the rule modality.

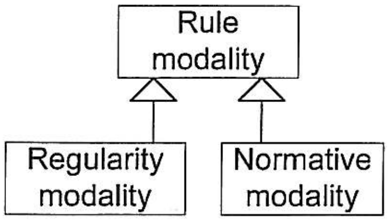

Figure 25 – Modalities

Based on the distinction of deontic norms and constitutive norms[13], we differentiate between different types of normative modality as illustrated in Figure 26. The primary distinction is the one between a deontic and a constitutive modality. This distinction is based on modal logic[5] and legal theory, e.g. Kelsen[23], Hart[10] and Eckhoff/Sundby[8].

Deontic modality: A deontic modality prescribes that the consequent scenario is obligatory, prohibited or permitted for an actor.

Obligation: If a scenario is obligatory, the addressee is required to cause it.

Prohibition: If a scenario is prohibited, the addressee is required not to cause it.

Permission: Permission is when a scenario is not prohibited.

Following standard deontic logic[31], the deontic modalities may be defined in terms of each other, i.e. to say that an action is obligatory is equivalent to say that it is not permitted not to perform the action. Similarly, if an action is prohibited, it is not permitted.

Constitutive modality: In a constitutive modality, the antecedent scenario counts as the consequent scenario.[1]

Constitutive norm is a term used by e.g. Herrestad ([13], p.142), but the same concept is referred to as qualification norm by Eckhoff/Sundby ([8], p.78), as secondary norm by Hart ([10], p. 94) or determinative rule by von Wright ([32], pp. 6-7).

A constitutive modality may e.g. indicate that a state (say an actor's age) counts as a specific role (here: adult), thereby "qualifying" the actor as a bearer of a role.

Authority: If a constitutive norm assigns authority, it qualifies an actor as a holder of a particular role that counts as authority.

If a constitutive norm assigns authority, it qualifies an actor as a holder of a particular role that counts as authority. Only an authorized actor may play this role. If an unauthorized actor endeavours to play the role in a given scenario (by behaving in the same way as an authorized actor), it means simply that a different scenario has taken place – ending in a different state where no legal effect has been achieved.

[1] In other words, the antecedent scenario is from a juridical perspective defined to be identical to the consequent scenario, and this definition or *qualification* [8] is legally binding. For example, the law may define that a verbal agreement (antecedent scenario) is qualified as (counts as) the signing of a written contract (consequent scenario).

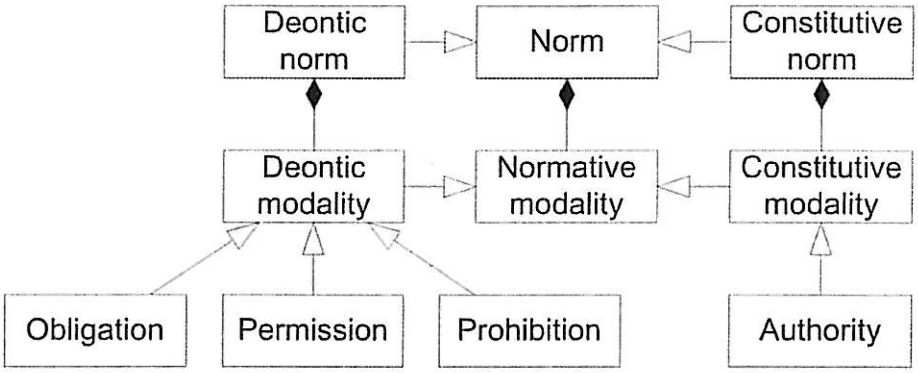

Figure 26 – Normative Modalities

Example 12

The eBay example involves norms with deontic and constitutive modalities:

The deontic norm prescribes that Billy and Sally are obliged to bring about the consequent action, should the antecedent scenario occur. The antecedent scenario of the norm obliging Billy to pay the camera is that he has, in a legally binding way (i.e. through the auction) agreed to pay for the camera. The consequent action is his compliance with the obligation, transferring the money to Sally as illustrated Figure 27.

Moreover, the applicable law may include the basis for a constitutive norm in a provision about the validity of a contract concluded in an auction, stating e.g. that the last bid before time-out *counts as* validly purchasing the item. Authority may also be relevant, e.g. with respect to who may validly sell the camera. The camera's sole owner will typically have the authority to sell his property. However, it will depend on the applicable law whether a sale by one of several owners, by a rightful possessor (e.g. a person hiring the object) or by a person with no possession rights (e.g. a thief) will count as valid. This means that if Sally lacks the authority to sell the camera, Billy may have purchased nothing.

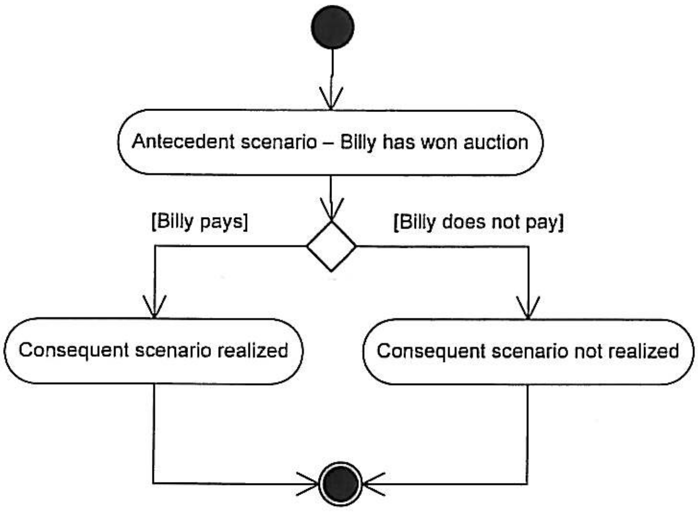
Antecedent scenario – Billy has won auction
[Billy pays]
[Billy does not pay]
Consequent scenario realized
Consequent scenario not realized

Figure 27 – Antecedent and consequent scenario of payment obligation

5.4 Sources of Norms

According to a theory developed by Ross[28], norms themselves need to be distinguished from the sources of norms.

Source of norm: The source of a norm is the fact, text, custom, etc. on which a norm is based.

Legal norms can be distinguished from social or ethical norms by reference to the way in which the norm binds the addressee, i.e. whether the norm is binding or non-binding. The formal distinction between a *legal norm* and another type of norm (social, ethical, moral etc.) is determined by whether the norm is based on *legal sources.*

Legal norm: A legal norm is a binding norm. A legal norm is based on a legal source.

Legal source: A source which in the relevant jurisdiction is considered to have legally binding force.

Non-binding norm: A norm which is based on non-binding source.

Non-binding source: A source that is not considered to have legally binding force.

A non-binding norm may e.g. be based on social standards or habits of actors in society (social norm), or on considerations about what is right and wrong (ethical norm), etc. We note that an action may be prescribed by binding and non-binding norms, concurrently.

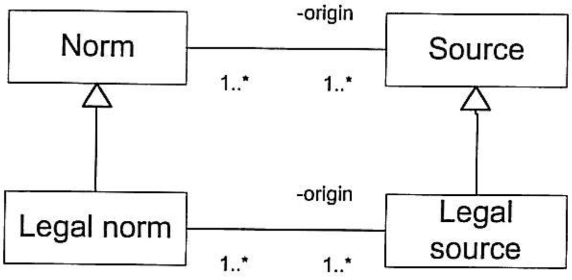

Figure 28 – Sources of norms

What is to be qualified as a *legal source* will thus partly be determined by the sources themselves, primarily those which (according to the same meta-norms) have a high rank according to the hierarchical structure of the legal system described by Kelsen[23]. There is no known instance of an exhaustive formalised list of such sources, therefore it will eventually have to be based on a consensus in the lawyer community, and the status of some types of sources may be contested (as are the decisions by first and appellate instance court decisions in Norway). Typically, the sources are the constitution, statutes, secondary legislation, decisions by supreme courts, and legal literature. The types vary between jurisdictions, for instance legislative history is a source used intensively in Norway, but generally not recognised in the United Kingdom.

The legal norm is based on the legal source, which is subject to interpretation. The process of interpretation may be trivial, reduced to a question of "reading" the texts. But it may also be more sophisticated, in which the doctrine on interpretation will govern the process. This is qualitatively different from "reading" or "understanding" a non-legal natural language text: for instance there will be norms governing the use of legislative definitions, inter- or intra-consistency between regulations, analogue reasoning *etc*.

Example 13

The interaction between Billy and Sally via eBay is subject to a number of norms of different types.

On the one hand, there will be concurrent social and legal norms obliging Billy to pay: Firstly there will probably be a non-binding social and ethical norm making payment obligatory. The source for this norm will be what is acceptable in society or what is considered as good behaviour according to ethical standards. Secondly, a legal norm will motivate Billy's actions. The source for the legal norm can be a legal text (e.g., if applicable, a provision like § 433 II of the German Bürgerliches Gesetzbuch, stating "The purchaser is bound to pay to the seller the purchase price agreed upon [...]"), together with other norms and taking into account the facts that Billy submitted his bid for the camera and won the auction.

The use of the eBay feedback forum, on the other hand, is subject to a non-legal norm, described e.g. by Keser[24]: The feedback about the other party should normally be very positive, and it is quite usual to add comments like "Excellent eBayer". The source of this norm would need to be a social expectation that can be observed amongst eBay users. We are not aware of any moral or legal norm obliging parties to exhibit this behaviour. However, as Keser observes, there seem to be economic incentives, which include the risk of negative counter-feedback by other users.

5.5 Normative Roles

There is a set of normative roles associated with norms and sources of norms. The authority to execute these rules is typically assigned by constitutive norms.

As illustrated in Figure 29, we distinguish between the norm addressee, its creator and an authority, which e.g. can enforce the norm. A part of the roles provided with authority reflect the classical separation of political powers of the judiciary, legislative and executive power represented in a political system, based on Montesquieu[26].

Authority: An actor with a specific power to create, to change, to implement or to enforce a norm.

Addressee: Any actor for whom a norm is binding.

Legislator: Actor entitled to create, modify or abolish a norm.

Executive: Actor responsible for implementing or executing a norm.

Judiciary: Actor responsible for making decisions based on norms, involving the interpretation, enforcement or other application the law. It is characteristic for this actor that the decisions are based on cases brought to the judiciary by other actors.

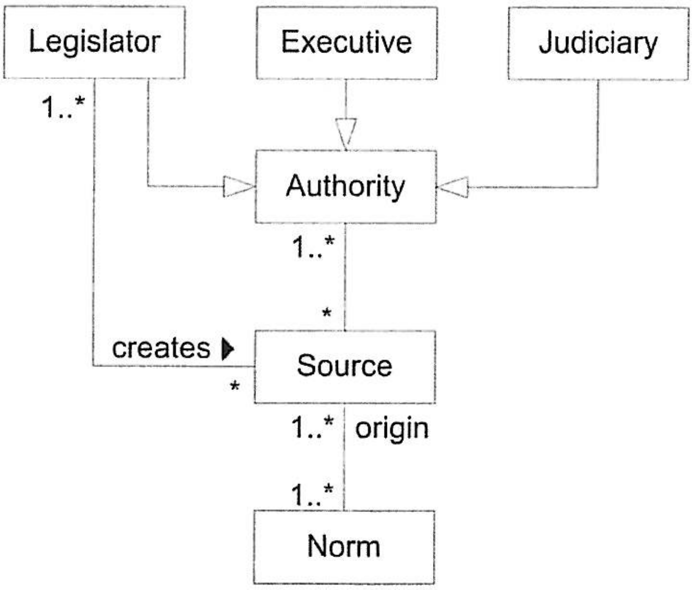

Figure 29 – Roles related to norm and its source

For roles related to *legal* norms, there is a constraint with respect to the types of actors who can assume a legally relevant role. The law only recognizes some actors, as depicted in Figure 30.

Legal actor: A legal actor is characterized by being related to a legal norm.

Juridical organisation[2]**:** An organisation that may be an addressee of a legal norm provided that the norm addressee is the organisation as such, not its individual members.

Note that organisations without legal personality and machines are not juridical organisations and are thus not considered legal actors. Such actors can consequently not assume legal roles. However, a participant in an organisation may be a legal actor, either in its quality as a juridical organisation, or simply as a human.

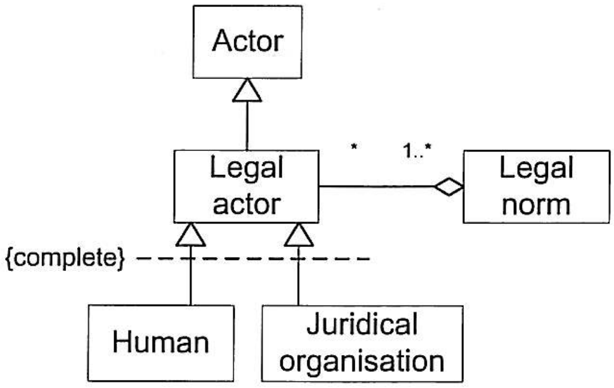

Figure 30 – Legal role

Example 14

Billy and Sally are humans and thus legal actors. eBay Inc. is a juridical organisation.

5.6 Contract

In principle, a contract is also a legal source, but of a different kind from the other legal sources mentioned above[25]. Most legal sources are based in the authority of the legal system. A contract, on the other hand, is based on the authority of the parties as legal actors, which have the freedom to bind themselves legally by accepting duties. The legal system will back this up by resources for enforcing the contracts, typically through the court system and executive authorities, in case of a violation with the contractual duties.

Contract: A contract is a mutually corresponding set of expressions of intent of two or more actors (the contractors), thereby creating a legal source.

The contractors have authority over the contract, including the power to enforce and (at least if acting jointly) change it. It is significant that a contractor is the addressee of the norm for which he or she has created the source.

Expression of intention: An action by which an actor expresses the intention to be bound by a contract.

Note that the expression of intention may take many forms, e.g. writing, oral, etc.

[2] In legal terminology, a juridical organisation is usually referred to as a legal person.

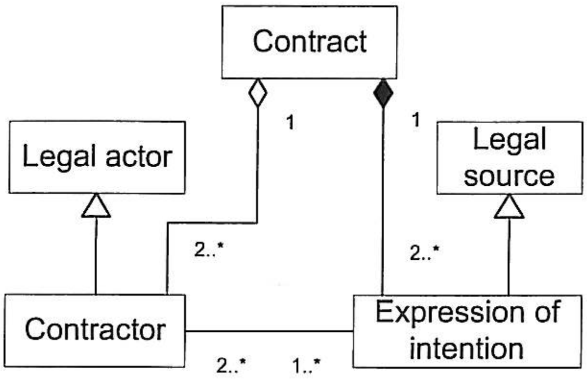

Figure 31 – Contract

Example 15

In the eBay example, there are several contracts. Firstly, there are respective contracts (user agreements) between eBay and its customers Sally and Billy regarding the participation in eBay. The contracts between eBay and its customers are concluded by the customers registering their accounts in eBay and accepting the eBay user agreement. Secondly, there is a contract (concluded through an auction) between the Billy and the Sally, governed by the applicable law. Figure 32 illustrates in a sequence diagram how the different contracts of relevance to the eBay scenario come into existence through communications between the involved actors.

The contract about the camera sale exists even though there may be no single written document. Only the legally relevant facts (a scenario) need to be present. In the event of a disagreement, these facts should however be documentable in order to meet the evidentiary requirements in the applicable law. The contract between Sally and Billy is concluded through the following scenario which has three characteristic elements:

- Sally's offer (through eBay), in which she describes the camera and defines some shipment conditions and
- Billy's bid for the camera, by which he accepts the shipment conditions and takes into account the camera description
- Billy being the bidder with the highest bid at timeout and thereby winning the auction.

The camera sales contract implies in principle that Sally has a shipment obligation subject to the shipment conditions specified in her offer. However, should these shipment conditions be contrary to a mandatory provision in the applicable law, the specific shipment condition may not be legally valid. Billy has a payment obligation, but according to the applicable law he may have the possibility to reclaim a part of his money, or even the full price, if the camera should not meet the standard specified by Sally.

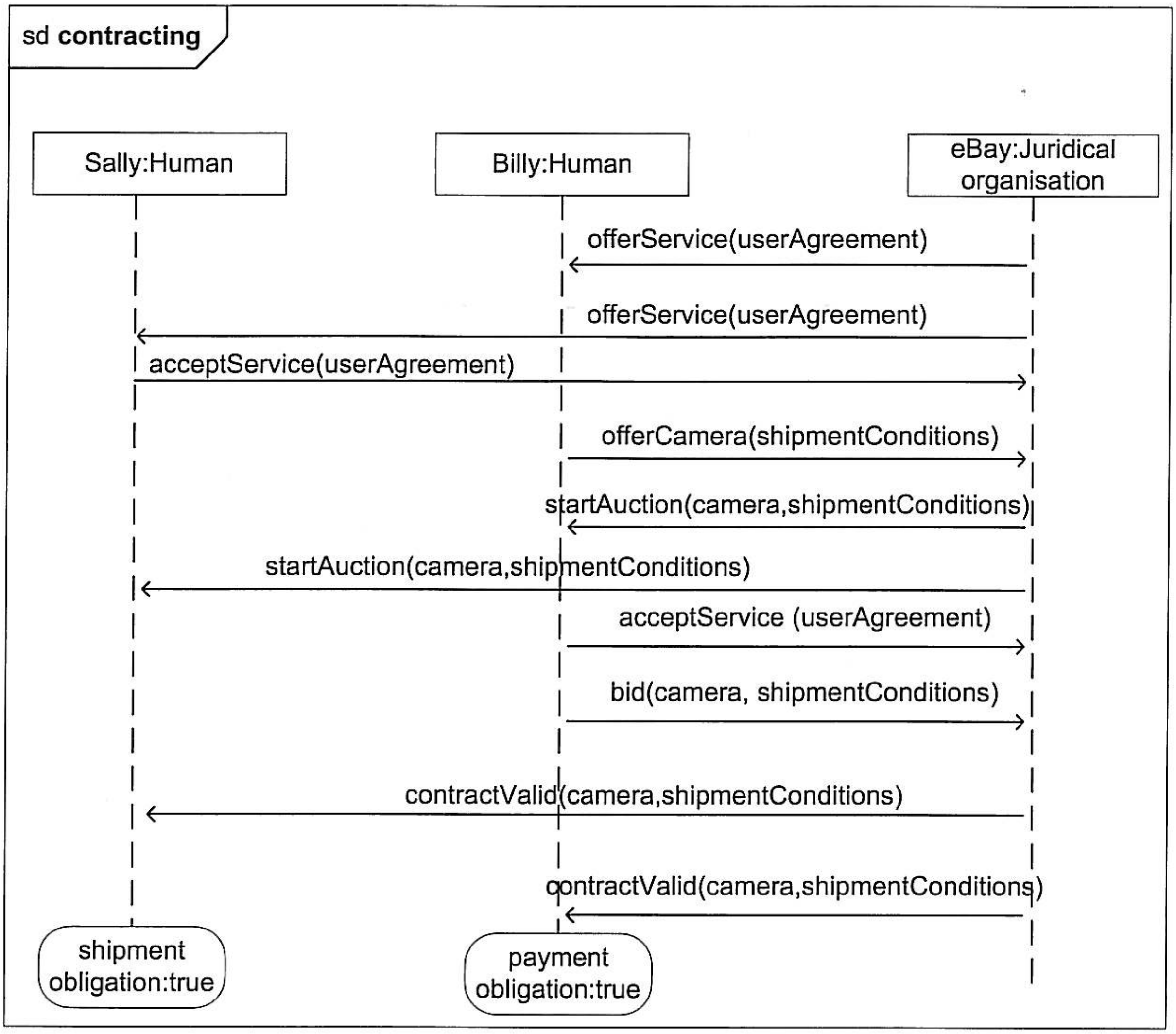
sd contracting
Sally:Human
Billy:Human
eBay:Juridical organisation
offerService(userAgreement)
offerService(userAgreement)
acceptService(userAgreement)
offerCamera(shipmentConditions)
startAuction(camera,shipmentConditions)
startAuction(camera,shipmentConditions)
acceptService (userAgreement)
bid(camera, shipmentConditions)
contractValid(camera,shipmentConditions)
contractValid(camera,shipmentConditions)
shipment obligation:true
payment obligation:true

Figure 32 – Contracting in eBay scenario

5.7 Legal risk

Norms can influence the value of the subjective concepts of risk and prospect. This is particularly the case with respect to legal norms, due to their binding force[25]. In order to exemplify this, we will address the special case of legal risk and legal prospect. Legal treatment as well as legal improvement may be modelled in a parallel way, but are omitted here.

Legal risk: A risk is a legal risk if its incident scenario involves a legal norm and if the norm has a significant impact on the risk value.

This is illustrated in Figure 33.

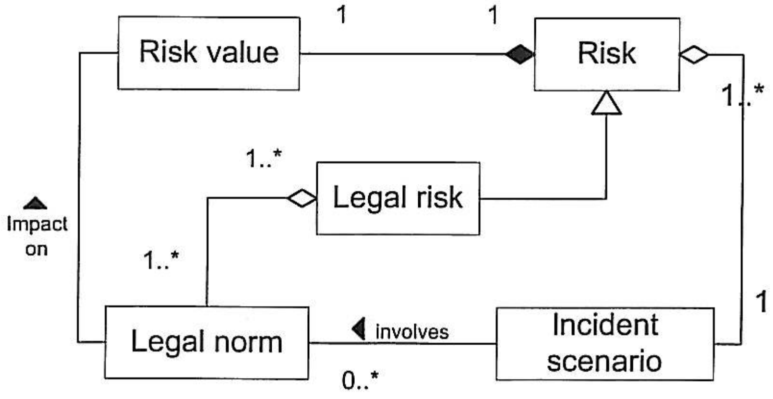

Figure 33 – Legal Risk

The norm's significant impact on the risk level means that the existence of the norm contributes to an increase in likelihood or the consequence value, or both. This is to say that without the norm, the risk value would be significantly lower.

Example 16

The eBay scenario may involve legal risks related to both deontic and constitutive norms:

Not paying the camera would be non-compliance with the payment obligation (a deontic norm), while payment as agreed will be compliance. If Billy chooses not to comply with his obligations, he may face the risk of having to pay compensation or being subjected to an enforcement action by an authority. In addition, Billy risks that a – costly – enforcement action by an authority would be legally permitted. Figure 34 depicts Sally's possibility to enforce the payment obligation through civil proceedings which may lead to coercion. Coercion would for example be the confiscation of monetary or other assets by the judiciary in order to fulfil the obligation against or without Billy's intention. In case Billy's action is considered a fraud, a report to an authority may even lead to a sanction like a fine or even incarceration. Sanction and enforcement action are both incident scenarios, since they involve an asset reduction with some likelihood. Both incident scenarios belong to legal risks: They involve legal norms permitting such actions, and these permissions have a substantial impact on the risk level.

A legal risk related to a constitutive norm would be that Sally is a minor who does not have the authority to sell her camera. The auction is void and Billy does not receive the camera. Without the (constitutive) norm negating minors' authority to participate in commerce, this risk would have zero likelihood.

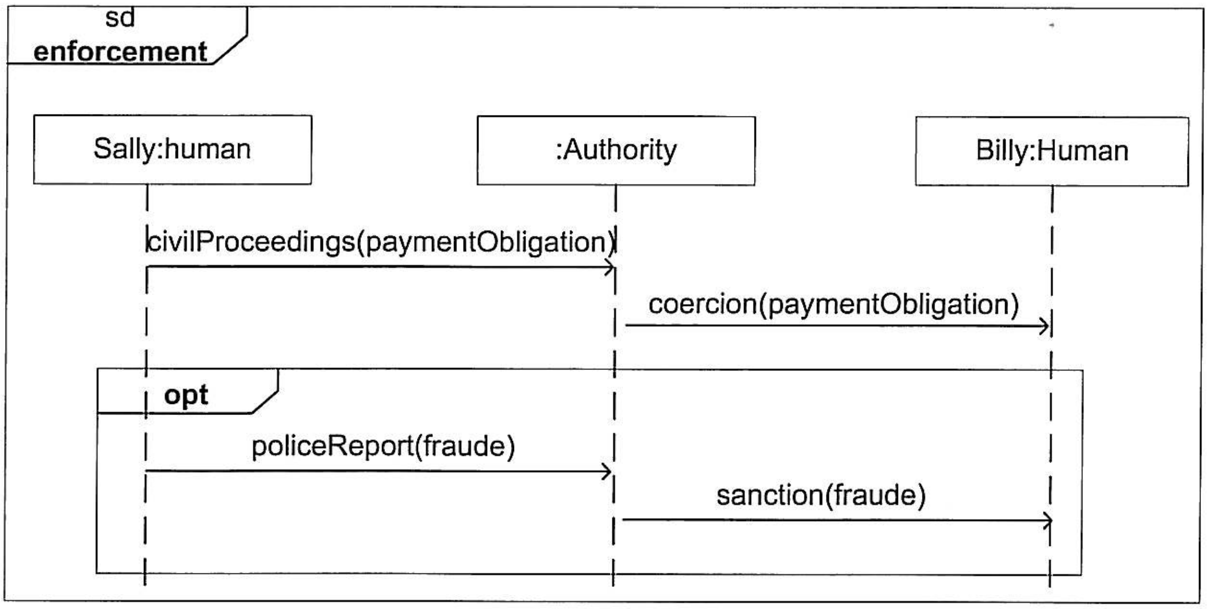

Figure 34 – Incident scenario related to enforcement of payment obligation

5.8 Legal prospect

Legal prospect: A prospect is a legal prospect if its opportunity scenario involves a legal norm and if the norm has a significant impact on the prospect value.

This is illustrated in Figure 35.

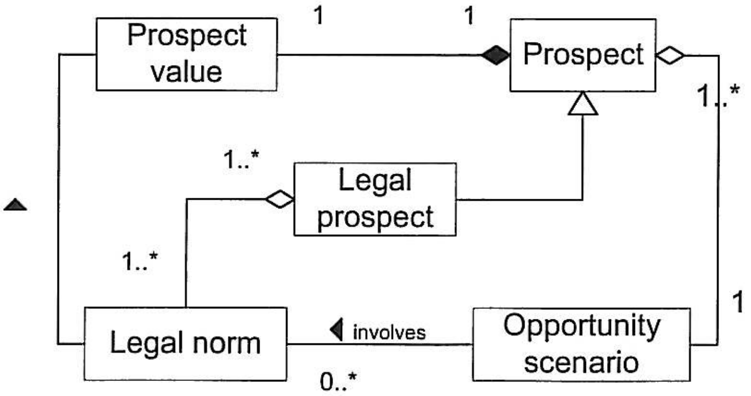

Figure 35 – Legal Prospect

Example 17

Billy's obligation to pay the camera (as specified above in Figure 32) is a prospect scenario for Sally. We assume that without a legal obligation, it is less likely that Billy will find it appropriate to pay any amount for the camera, and if he did pay, the amount could be significantly lower. Hence, without the legal obligation, the prospect value would be significantly lower.

5.9 Policy

Policies may be understood as particular sets of rules that are defined for the purpose of regulating the behavior of an organization or a computerized system within an organization. These rules are typically defined, implemented and enforced by the organization itself. Our definition of a policy is based on the widely accepted definition by Damianou et al [1].

Policy rule: A policy rule is a deontic norm that defines a choice in the behavior of the target.
Policy: A policy is a set of policy rules.

Notice that we here understand the term "system" quite generally as a term denoting both organizations and machine systems. Figure 36 shows the class diagram for the concept of policy.

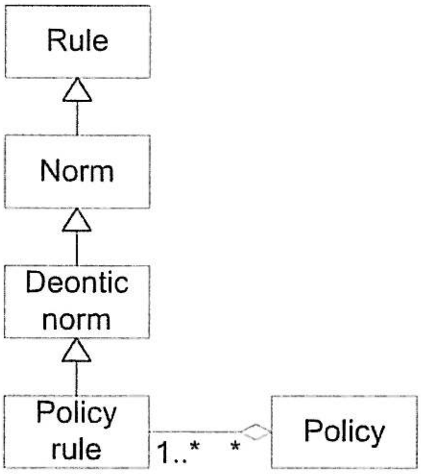

Figure 36 – Policy

6 Trust

Trust is a concept which is used in many different contexts, with various meanings. We are basing our definition of trust on Gambetta[9], whose definition is well established within trust management, see e.g. Jøsang[20]. In this section we rephrase this definition in terms of our previously defined notions, and relate the definition of trust to other central concepts like risk and assurance.

Trust: Trust is the *subjective probability* by which an actor, the trustor, expects that another entity, the trustee, performs a given transition on which its welfare depends.

Thus defined, trust is a belief of the trustor regarding the future behaviour of the trustee. Since trust is a belief it is a subjective notion. We will refer to low levels of trust as *distrust*.

Often the trustor only expects the trustee to perform a given transition, if certain conditions are present. Such conditions may be described in a scenario, which in Figure 37 we have denoted an *antecedent scenario*.

The trustor's welfare is an intrinsic part of our notion of trust which is modelled by the relation between transition and asset. If the trustee performs as expected, the trustor anticipates an increase of asset value, or perhaps that existing assets are not harmed. On the other hand, by trusting the other entity, the trustor places the trustee in a position where the latter can impose harm to one or more of the trustor assets by not performing as expected. These possibilities of increase or decrease of asset values are what constitute the aspects of prospect and risk respectively in a trust relation.

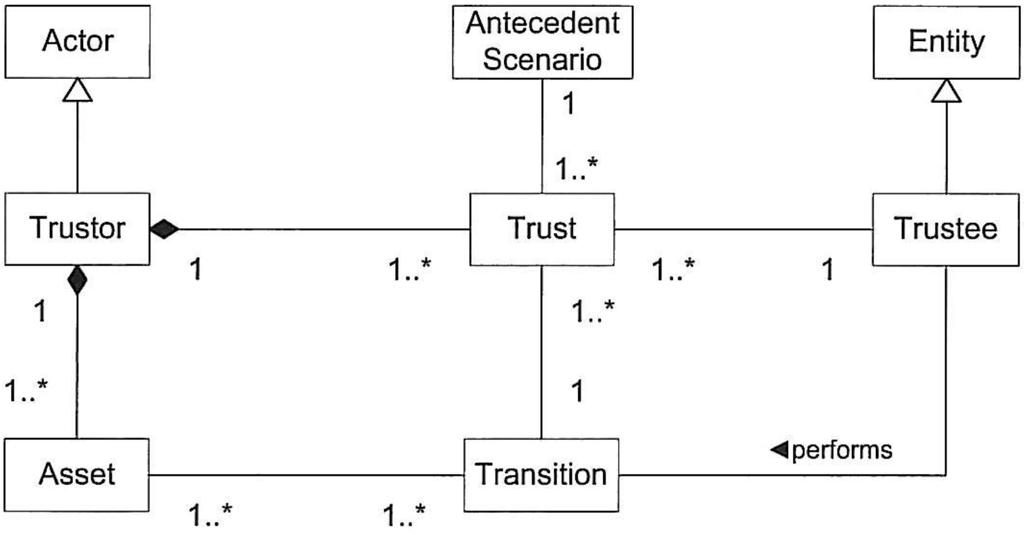

Figure 37 – Trust

In order to be able to speak about the world as it actually is, as opposed to how it is perceived, we introduce the concept of trustworthiness as the objective counterpart to the subjective notion of trust.

Trustworthiness: Trustworthiness is the *objective probability* that an entity, the trustee, performs a given transition on which the welfare of an actor, the trustor, depends.

Trustworthiness may sometimes be described by a *regularity* (see Figure 21), in which the antecedent scenario describes the circumstances in which the trust applies, the regularity modality is the objective probability, and the consequent scenario is the transition in question.

Often a trust relation will be governed by a norm, i.e. there will be a normative obligation for the trustee to behave trustworthy. In that case, a violation of trust may rightfully lead to sanctions by proper authorities. In many cases, the trustee has hence an interest in acting as trustworthy.

Example 18

Figure 38 shows interactions between Sally and Billy in which trust is relevant. The diagram is an alternative to the specification of the auction given in Figure 13. The trust relation concerns whether or not Sally will ship the camera after receiving the payment. The payment of the camera defines the antecedent scenario of the trust relation. Given that the antecedent scenario is fulfilled (the payment has been received) Billy has a certain level of trust in that Sally will ship the camera. By using an alternative fragment we illustrate the fact that Sally may choose not to ship the camera. Thus, Billy's trust is the probability by which he expects that Sally performs the shipment.

The attribute values shown in the diagram describe asset values at various times of the scenario. Note that if Billy receives the camera, its value will not necessarily be above zero. The exact value of the camera will be determined by the condition it is in at the time of arrival.

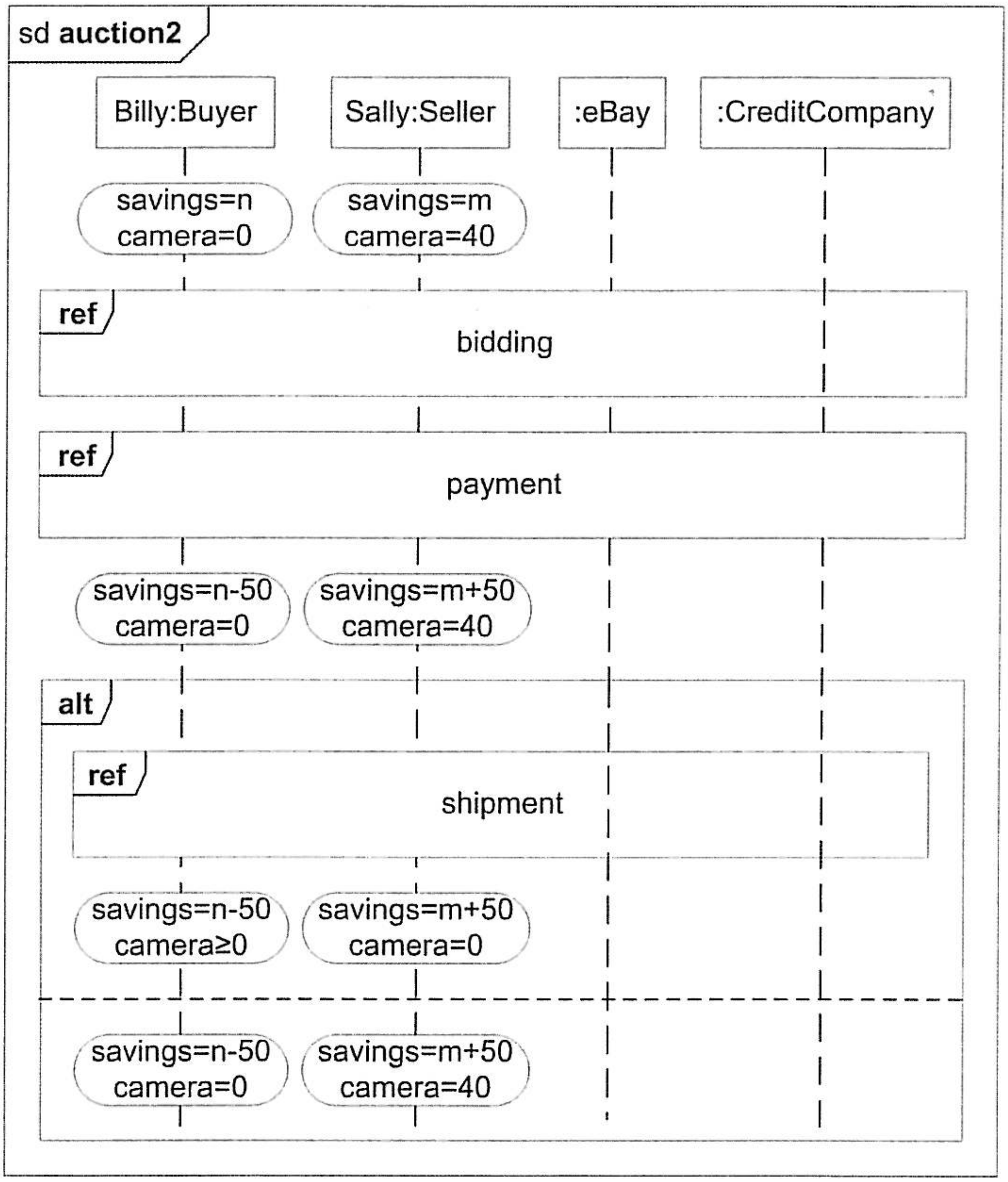

Figure 38 – Behavior options

6.1 Trust and Risk

In this section we describe the relationship between trust and risk. We focus on two main aspects. Firstly, a direct relation in which the actions of the trustee directly defines an incident scenario. Secondly, an indirect relation in which the actions of the trustee may indirectly lead to an opportunity scenario.

Example 19

The diagram in Figure 38 describes an incident scenario related to the assets of Billy. We observe that from Billy's point of view the payment of the camera constitutes a threat scenario, which may lead to an incident scenario. The unwanted incident occurs if Sally does not ship the camera, which will consequently never be received. This constitutes a risk to Billy's combined assets.

Since the actions of Sally directly define the incident scenario, the likelihood of the risk will be directly related to the objective likelihood of Sally performing the shipment.

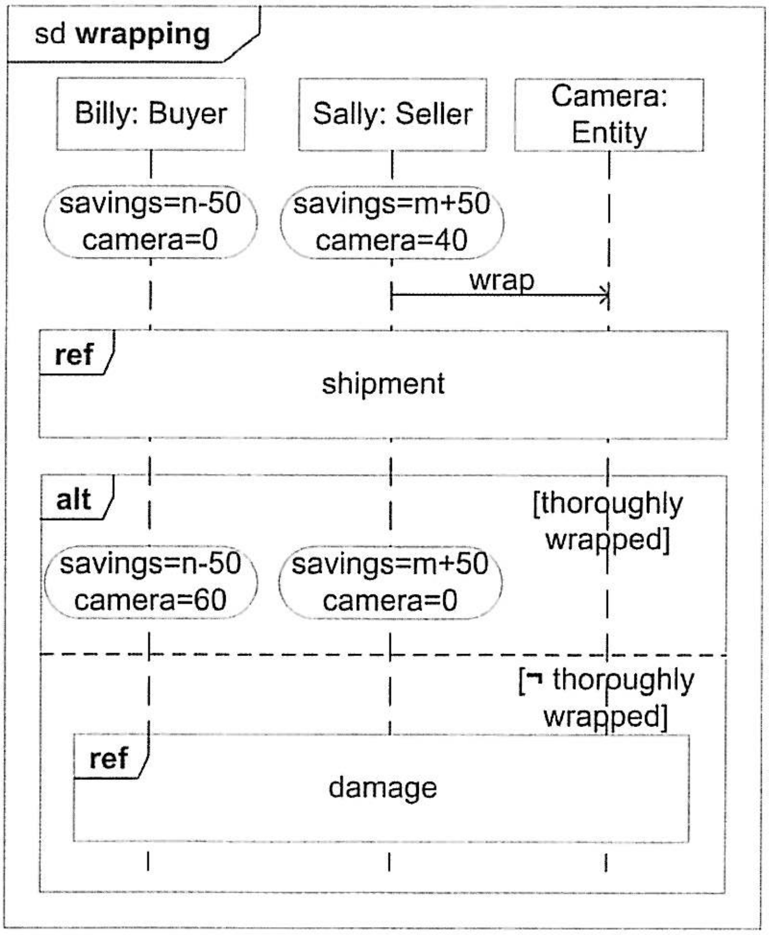

Figure 39 – Wrapping of Camera

Example 20

As noted above, the value of the camera to Billy depends on its state at time of arrival. If, for example, the camera is not thoroughly wrapped, it may be damaged during transport. Hence, an important aspect of the transaction is the level of trust Billy has in the wrapping-capabilities of Sally. In Figure 39 we illustrate how thorough wrapping by Sally will lead to the camera being received undamaged. This scenario constitutes an opportunity scenario for Billy. We observe that in this case, the actions of the trustee (the wrapping performed by Sally) are indirectly related to the positive consequences, the prospect, of receiving the camera. Hence, the likelihood aspect of the prospect is not directly related to the trust Billy has to Sally performing a thorough wrapping. Figure 40 shows the possible scenarios in case the camera has not been thoroughly wrapped.

Concerning the wrapping transition performed by Sally, it should be noted that it is not exclusively specified in terms of the state of the trustee, but includes the 'outcome', i.e. the state of another entity: the camera.

Since a collaboration often involves several trust relations, the decision to trust must be based on comparison of the potential negative and positive effects of entering the collaboration. We observe that this comparison is more difficult to perform if the actions of the trustee are indirectly related to risks and prospects of the collaboration.

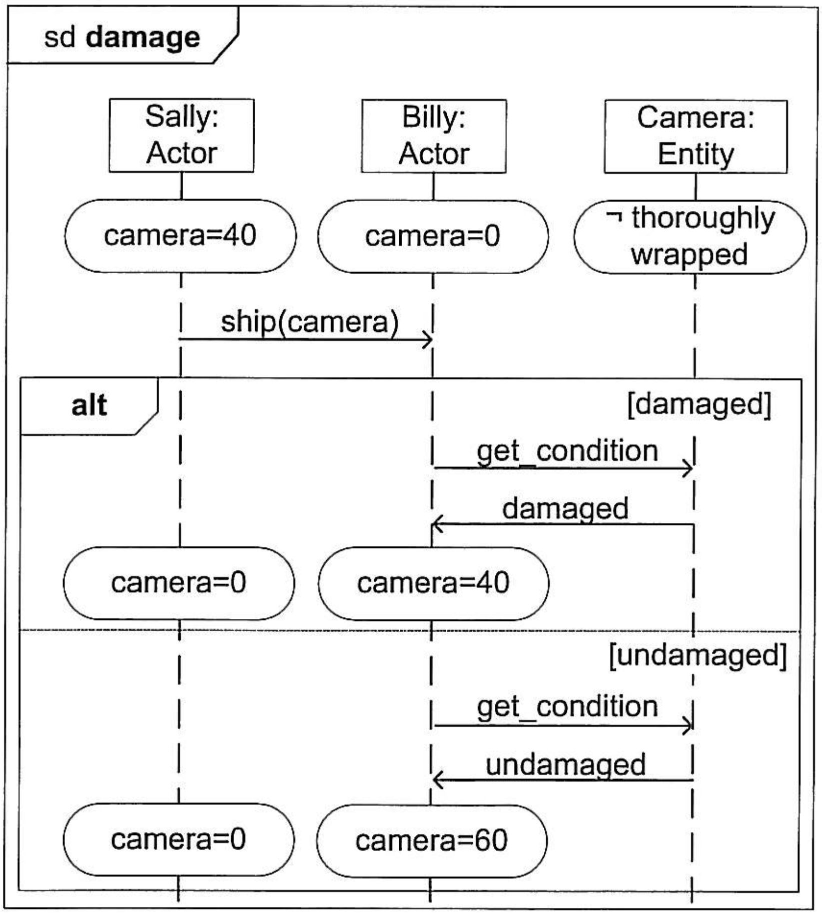

Figure 40 – Damage during shipment

6.2 Trust and Assurance

In this section we relate the inherent uncertainty of trust assessment to the notions of assurance and confidence. Above, we defined trust as a 'subjective probability'. Hence, trust may be represented by a single probability value. However, in our model we also provide a refinement of this notion by the concept of confidence.

Confidence: The perceived certainty of an estimate or statement.

Thus, the level of trust may be modelled by an estimated probability together with a confidence measure of the estimated probability.

Within the information security field, the Common Criteria methodology[6] relates the concept of confidence to the concept of assurance, by defining assurance as the grounds for confidence that an entity meets its security objectives. In order to be able to relate the notion of assurance to the notion of trust, we define assurance in a more general way.

Assurance: Grounds for confidence in an estimate or statement.

Hence, a high level of assurance means that there are good grounds for confidence in an estimate or statement. With regard to trust, we will refer to high levels of assurance as well-founded trust.

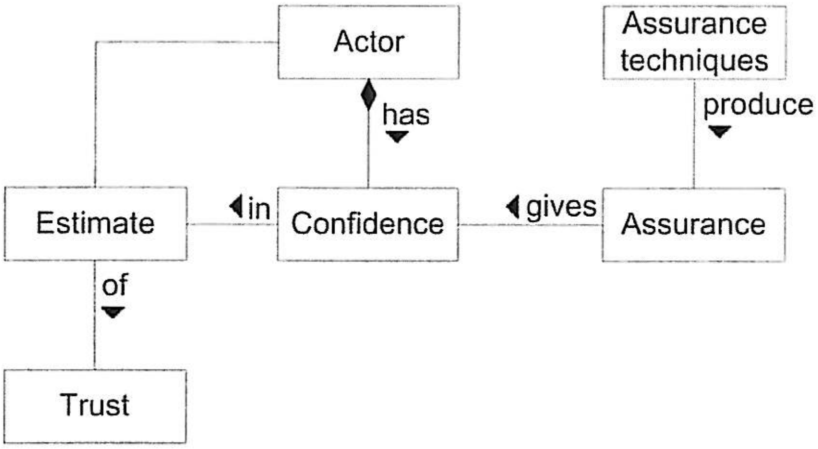

Figure 41 – Confidence and trust

In Figure 41 the relation between trust, confidence and assurance is modelled. Within trust analysis we expect confidence to be relevant when deciding whether further evidence, and hence assurance, is needed for a particular assessment. For example, the stakeholders may require a higher level of assurance and confidence, when making decisions concerning scenarios with high consequences.

Hence, we believe that an important aspect of trust analysis is to use information about a trustee as a source of assurance, and hence as grounds for confidence and trust.

Example 21

Suppose, Sally has only a few previous transactions on eBay and that they are all positively rated, then Billy may assess that there is a high probability that Sally will send the camera. However, Billy may not be very confident in this assessment. On the other hand, if Sally has many positive previous transactions, and some of these are with Billy, then Billy may be very confident in his high probability assessment of Sally sending the camera.

Such a high confidence may be a necessary condition for Billy being willing to engage in bidding for the camera, if it is a very valuable camera.

7 Conclusion

When trust management addresses trust issues from the perspective of the trustor, the activity of assessing the trustworthiness of potential and actual trustees and make decisions on that basis is crucial. From the perspective of the trustee, trust management is about increasing the perceived trustworthiness of the trustee, or at least ensure that the trustworthiness is correctly represented. In both cases there are a number of issues involved that should be considered.

A basic aspect of trust that is widely discussed in state-of-the-art literature on trust management is the aspect of risk. For the trustor it is important to understand the risks involved in transactions involving trust and to try to mitigate unacceptable risks, whereas the trustee might have interest in being perceived as a transaction partner the collaboration with which involves low risks. A typical example of the latter is a business enterprise that needs good customer and business relations.

In addition to define and clarify the notion of risk, we have in this document emphasized the dual notion of prospect to the same extent. In order to understand the dynamics of trust, the relation between trust on the one hand and risk and prospect on the other must be accounted for. The decision to trust inevitably involves the acceptance of a certain level of risk, and the motivation for this risk acceptance often stems from a perceived prospect.

Trust relations can be very complex and there may be a variety of factors involved in the making, maintenance and breaking of trust relations. Security, risk and prospect surely affect trust relations, and are in turn related to legal issues; laws and contracts can contribute to increase security, mitigate risks, increase prospect and ensure trust, but legal norms can also pull in the other direction by introducing legal risks or restricting the access to implement security issues. Norms are strongly related to trust as they often serve as the basis upon which trust is built, be it social, ethical or legal norms or a combination of the three.

The ENFORCE project brings together the disciplines of computer science, law, philosophy and social sciences with the aim of approaching trust issues from many perspectives. In this document we have established a conceptual basis for trust management that introduces and relates notions from the different disciplines. The conceptual framework serves as a conceptual basis for the ENFORCE research, ensures a common understanding of the various notions and establishes a context for the ENFORCE research.

8 References

[1] AS/NZS 4360:2004, Risk Management, 2004

[2] den Braber, F., Hogganvik, I., Lund, M. S., Stølen, K. and Vraalsen, F.: *Modell-based security analysis in seven steps – a guided tour to the CORAS method.* To appear in BT Technology Journal, Springer, 2007

[3] Bresciani, P., Giorgini, P., Giunchiglia, F., Mylopoulos, J. and Perini, A.: *Tropos: An Agent-Oriented Software Development Methodology.* In Journal of Autonomous Agents and Multi-Agent Systems 8(3), pp. 203-236, 2004

[4] Castro, J., Kolp, M. and Mylopoulos, J.: *A Requirements-Driven Development Methodology.* In CAiSE'01: Proceedings of the 13th International Conference on Advanced Information Systems Engineering, LNCS 2068, pp. 108-123, Springer, 2001

[5] Chellas, B. F. *Modal Logic, an Introduction*, Cambridge: Cambridge University Press, 1980

[6] Common Criteria for Information Technology Security Evaluation. Version 2.3, August 2005, www.commoncriteriaportal.org

[7] Damianou, N., Dulay, N., Lupu, E. and Sloman, M.: *The Ponder Policy Specification Language.* In Proceedings of Policy 2001, Workshop on Policies for Distributed Systems and Networks, LNCS 1995, pp. 18-39, Springer, 2001

[8] Eckhoff, T. and Sundby, N. K.: *Rechtssysteme. Eine systemtheoretische Einführung in die Rechtstheorie,* Berlin 1988

[9] Gambetta, D.: *Can We Trust Trust?* In Gambetta D. (ed.): *Trust: Making and Breaking Cooperative Relations*, pp. 213-238, Basil Blackwell, Oxford, 1990

[10] Hart, H. L. A.: *The Concept of Law*, Oxford 1994

[11] Haugen, Ø., Husa, K. N., Runde, R. K. and Stølen, K.: *STAIRS towards formal design with sequence diagrams.* In Software & System Modeling, pp. 1-13, 2005

[12] HB231, Information Security Risk Management Guidelines, Standards Australia/Standards New Zealand, 2004

[13] Herrestad, H.: *Formal Theories of Rights*, Oslo 1996

[14] Hogganvik, I. and Stølen, K.: *A Graphical Approach to Risk Identification, Motivated by Empirical Investigations.* In MoDELS 2006, LNCS 4199, pp. 574-588, Springer, 2006

[15] ISO/IEC 13335, Information Technology – Guidelines for Management of IT Security, 2000

[16] ISO/IEC FCD 15414: Information Technology – Open Distributed Processing – Reference Model – Enterprise Viewpoint, 2000

[17] ISO/IEC 17799:2000(E), Information Technology – Code of Practice for Information Security Management, 2000

[18] ISO/IEC 15408:2005, Information technology – Security techniques – Evaluation criteria for IT security, 2005

[19] Jones, S., Wilikens, M., Morris, P. and Masera, M.: *Trust Requirements in E-business.* Communications of the ACM, 43(12) pages 81-87, 2000

[20] Jøsang, A., Keser, C. and Dimitrakos, T.: *Can We Manage Trust.* Proceedings of the 3rd International Conference on Trust Management, iTrust 2005, LNCS 3477, pp. 93-107, Springer, 2005

[21] Kahneman, D. and Tversky, A.: *Propsect Theory: An Analysis of Decision under Risk.* Econometrica, vol. 47, No. 2, pp. 263-292, 1979

[22] Kant, I.: *Kritik der reinen Vernunft,* Berlin 1998

[23] Kelsen, H.: *Pure Theory of Law*, London 1960

[24] Keser, C.: *Experimental games for the design of reputation management systems*, IBM Systems Journal, Vol. 42, No. 3, pp. 498–506, 2003

[25] Mahler, T., Bing, J.: *Contractual Risk Management in an ICT Context -- Searching for a Possible Interface between Legal Methods and Risk Analysis.* Scandinavian Studies in Law, Vol. 49, pp. 339-357, 2006

[26] Montesquieu, C. d. S.: *The Spirit of laws / Charles de Secondat, Baron de Montesquieu;* translated by Thomas Nugent, 1752, (2001)

[27] Object Management Group: *Unified Modeling Language*, www.uml.org/

[28] Ross, A., *Theorie der Rechtsquellen : ein Beitrag zur Theorie des positiven Rechts auf Grundlage dogmenhistorischer Untersuchungen*, Leipzig 1929

[29] Vraalsen, F., Lund, M. S., Mahler, T., Parent, X. and Stølen, K.: *Specifying Legal Risk Scenarios Using the CORAS Threat Modeling Language.* Proceedings of the 3rd International Conference on Trust Management, iTrust 2005, LNCS 3477, pp. 45-60, Springer, 2005

[30] von Neumann, J. and Morgenstern, O.: *Theory of Games and Economic Behavior,* 1953 edition, Princeton, NJ: Princeton University Press, 1953

[31] von Wright, G. H.: *Deontic Logic.* Mind 60, pp. 1-15, 1951

[32] von Wright, G. H.: *Norm and Action, A Logical Enquiry*, London 1963