Deliverable

15

Report on Legal Issues

WP9 Legal Issues

Tobias Mahler(ed.),
NRCCL

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

LEGAL NOTICE

The following organisations are members of the Trustcom Consortium:

Atos Origin,
Council of the Central Laboratory of the Research Councils,
BAE Systems,
British Telecommunications PLC,
Universitaet Stuttgart,
SAP AktienGesellschaft Systeme Anwendungen Produkte in der Datenverarbeitung,
Swedish Institute of Computer Scence AB,
Europaeisches Microsoft Innovations Center GMBH,
Eidgenoessische Technische Hoschschule Zuerich,
Imperial College of Science Technology and Medicine,
King's College London,
Universitetet I Oslo,
Stiftelsen for industriell og Teknisk Forskning ved Norges Tekniske Hoegskole,
Universita degli studi di Milano,
The University of Salford,
International Business Machines Belgium SA .

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: Analysis of Legal Issues

Work Package: 9

Task:

Document title: Report on Legal Issues

Version: 1.0

Document reference:

Official delivery date: 31 July 2005

Actual publication date: 30 July 2005

File name:

Type of document: Report

Nature: Public

Authors: Jon Bing[1], Dana Irina Cojocarasu[1], Andrew Jones[2], Mass Soldal Lund[3], Vebjørn Iversen[1], Tobias Mahler[1], Thomas Olsen[1], Xavier Parent[2], Bjørnar Solhaug[3], Ketil Stølen[3], Fredrik Vraalsen[3]

Reviewers: CCLRC and Atos Origin

Approved by:

Version	Date Date	Sections Affected
V 1.0	31/07/05	Final version

---

[1] NRCCL

[2] KCL

[3] SINTEF

Table of Content

1 EXECUTIVE SUMMARY

This report summarises the research performed in TrustCoM work package 9. The objective of TrustCoM's legal work package is to study selected legal issues in relation to trust, security and contract management for virtual organisations. The present study's focus is on the legal risks that may arise for participants in VOs, based on the test bed scenarios developed in TrustCoM. Legal risk analysis allows this study to have a proactive approach on legal issues, which can be seen as opposed the reactive perspective inherent in traditional legal methods. Moreover, legal risk analysis facilitates the integration of the perspectives of trust and security with the focus on legal issues related to virtual organisations.

This work contributes to the overall TrustCoM framework by defining some basic legal requirements for trust, security and contract management in VOs. Moreover, the legal group has closely collaborated with other TrustCoM partners, in particular in relation to the TrustCoM scenarios on collaborative engineering and e-learning. These scenarios were analysed and discussed with TrustCoM partners in order to identify the types of contractual relations that need to be in place in order to make the VO scenarios operable. These contractual relations were used as bases for more detailed legal analyses.

The study applies legal risk management as a novel methodology to analyse legal issues related to trust, security and contracts in VOs.

Since legal issues largely depend on the specific context, including the nature of the collaboration and its purpose, the research mainly focuses on issues of relevance to the scenarios selected by the project. The legal research presented in this report falls into the three categories data protection law, intellectual property law and international issues. Within these categories, more specific legal issues were selected based on relevance for the TrustCoM project, including the scenarios and the on-going technical development work related to trust, security and contract management.

With respect to the **collaborative engineering scenario** the legal risk analysis focuses on intellectual property rights and confidentiality. The risk analysis results indicate how legal risks, such as the loss of protection of confidential information, can be treated by an integrated solution, including contractual elements, trust management and security management. The contractual treatments should consist in an adaptation of a contract template to the specific risks identified in the scenario. The legal risk analysis provided some first indications about how a confidentiality clause can be adapted to the specific scenario. Since the graphical representation implies a simplification, a lawyer would have to integrate analysis results into the contractual document in an appropriate way, taking into account the terminology and the system of the contractual template. This indicates the need for a more detailed analysis of confidentiality clauses in VO contracts.

The legal analysis of the **AS / eLearning scenario** focused on legal risks related to international issues, i.e. choice of law and jurisdiction. While the international nature of a VO has few implications for the computational infrastructure of a VO, it is a

factor of major importance in a legal context. However, most of the identified legal risks relating to international issues may be mitigated by defining an exclusive jurisdiction and an applicable national law in VO-related contracts. The remaining legal risks, particularly in relation to consumer contracts, should be tolerable and relate to the special protection for consumers. Future work in relation to the E-Learning scenario will focus more on the analysis of legal issues related to the access to digital content, and how the computational access may be integrated with the contractually agreed access.

The utilisation of an UML-based graphical language in the legal risk analyses ensured compatibility of the legal study with other work in TrustCoM. The latter language was extended with legally relevant concepts, in order to make it more suitable for the analysis of legal issues. Moreover, the formal elements in the language make it more precise and facilitate the development of automated tools for processing the graphical models.

This report consists of a rather short main part and five appendices which can be consulted for more detailed information.

- Appendix A describes the results of the legal risk analysis of the CE scenario with respect to intellectual property rights. These results are summarised in Section 3 of this main report.
- Appendix B includes the analysis of international issues (choice of law and jurisdiction), based on the AS / eLearning scenario, summed up in Section 4 of this report.
- Appendix C refers the results of the analysis of legal issues related to data protection law, summarised in Section 5 of this report.
- Appendix D and E regard respectively the conceptual model and the graphical language for legal risk analysis, which also are discussed in Section 7 of this main report.

Hence, most sections of this main report are further detailed in the appendices. Only section 6, which discusses legal requirements to trust, security and contract management, does not correspond to a separate appendix. This is due to the fact that Section 6 on the one hand is based on some of the findings of the legal risk analyses detailed in Appendices A to C, and on the other hand includes additional legal requirements, which have not been studied in detail, but which nevertheless are summarized, since they may have consequences for trust management, security management and contract management for virtual organisations.

2 INTRODUCTION

The objective of the TrustCoM project is to develop a trust and contract management framework enabling secure collaborative business processing within secure, scalable highly dynamic, integrated and targeted virtual organisations, which are formed on-demand, are self-managed and share services, resources, information and knowledge across enterprise boundaries, in order to tackle collaborative projects that their participants could not undertake individually. Such VOs will be based on new forms of collaboration in which participants can specify and negotiate their own conditions of involvement by means of electronic contracts whose operation is supported and enforced by the computing infrastructure.

TrustCoM's approach needs to take into account both technical and non-technical, including legal, aspects of trust and security. Neither trust nor security are legal terms, even though security is addressed e.g. in the field of information security law and trust is a core value protected by both statutory laws and contracts. Not even virtual organisation is a legal term. From a legal point of view, the concept of VO describes a complex multi-participant contractual situation, and many of the legal challenges depend essentially on the nature of the collaboration that is to be covered by the contracts.

The objective of TrustCoM's legal work package is to study selected legal issues in relation to trust, security and contract management for virtual organisations. This study was performed by a group of researchers that consists of lawyers, computer scientists and philosophers with a background in formal methods. This combination of skills and backgrounds allows the team to perform the research with an interdisciplinary perspective on legal issues.

We should not omit some of the challenges we have faced during the study: The research started with rather abstract legal questions which were not really tied into the project. Furthermore, on the one hand, the legal research has an important role to play in eliciting the legal constraints that do or should define the use of the applications developed by other TrustCoM participants. This would normally indicate that the legal research should be of a rather general nature – more similar to legal counselling done by a law firm – covering the main topics of relevance to the project. On the other hand, the legal work performed in the project should fulfil scientific criteria, in particular novelty, requiring focus on very specific and detailed legal issues.

This study attempts to strike a balance by providing some more general requirements to trust, security and contract management and by selecting more specific legal issues based on the scenarios developed by the TrustCoM project, in addition to introducing legal risk analysis as a novel inter-disciplinary approach for studying these legal issues. Legal risk analysis allows this study to have a proactive approach on legal issues, which can be seen as opposed the reactive perspective inherent in traditional legal methods. Moreover, legal risk analysis facilitates the integration of the perspectives of trust and security with the focus on legal issues related to virtual organisations.

The following subsections will provide more details on both the selection of specific legal issues and on the relevance of legal risk management for addressing trust, security and contracts in VOs.

2.1 Selection of Legal Issues

The legal research presented in this report covers issues in three areas, namely data protection law, intellectual property law and international issues. Within these areas, more specific legal issues were selected based on relevance for the TrustCoM project, including the scenarios and the on-going technical development work related to trust, security and contract management.

- In an initial study, data protection law was analysed in relation to trust, with a particular view on reputation systems. This was discussed in the context of one of the initial TrustCoM scenarios.
- The second study focused on one of the two TrustCoM testbed scenarios, i.e. the collaborative engineering scenario. The protection of confidential information, i.e. trade secrets and know-how was identified as the most relevant issue in this scenario. Hence, a detailed analysis was performed in order to identify related legal risks and respective treatments, and more research should be conducted in relation to confidentiality issues.
- The third study concentrated upon the TrustCoM e-learning testbed scenario. An initial analysis of the scenario revealed the relevance of a number of different legal issues. Firstly, the scenario describes collaboration between businesses from different countries, and the relation of these contracts to jurisdictions and national laws needed to be clarified. Secondly, the scenario describes a distributed system for accessing digital content on an e-learning marketplace. In this context it will be relevant to discuss how the technological access management can be integrated with respective contracts, and what kind of liability risks arise when there is a conflict between the contractually foreseen access and the technological access level. The present study is confined to the analysis of legal risks related to choice of law and jurisdiction, an issue which also has been raised from other partners working on the TrustCoM conceptual models. Legal issues related to access to digital content will be addressed in further work.

2.2 Methodology – Legal Risk Analysis

A recently published *strategic roadmap for advanced virtual organizations* points out that the analysis of legal risks arising in operating virtual organizations and the development of legal strategies to overcome them is an important research task in

order to support collaborative networked organizations.[4] Hence, the present study's focus is on the legal risks that may arise for participants in VOs, based on the test bed scenarios developed in TrustCoM. The following sections describe this study's methodological approach, i.e. legal risk analysis.

2.2.1 A proactive approach to legal issues

The present study's focus on legal risk analysis is motivated by a proactive approach to legal issues, seeking to identify probable future legal problems and looking for strategies to mitigate these. This proactive approach can be seen as opposed to the more traditional reactive focus of legal analysis, which has concentrated on determining the law once a problem has occurred. While a proactive legal analysis also includes elements which merely focus on determining the law, it also needs to deal with a partly unknown future and with clients' wishes to protect their assets in this future. The proactive perspective is in itself not new; lawyers have provided future-oriented legal advice for a long time. However, when analysing legal issues related to trust, security and contract management in VOs, we need to address legal risks in the context of the technological framework that will be used by VOs, and existing legal methods provide only limited guidance in this context.

Hence, when deciding the methodological focus of this study, we needed to direct our attention towards risk analysis methods developed in other disciplines, in order to assess their suitability for the legal domain. Risk analysis has been developed and utilized in other disciplines including engineering, information security and financial investment, which all deal with risks that can be identified, analysed and treated in a structured way. The term risk analysis is closely related to risk management, which consists of a series of risk analyses. Risk management is in other disciplines understood as the set of coordinated activities to direct and control an organisation or system with regard to risk. Risk management with a focus on legal issues can thus enable us to view legal risks as a part of a broader picture of risks, incorporating e.g. trust and security and to identify integrated treatments. Risk analysis methods from the information security domain are of particular interest to this study, because they are concerned with risks in relation to information and information systems, which are of high relevance to TrustCoM.

2.2.2 Risk Analysis Related to Trust

Risk analysis is not only related to security, but also to trust. When focusing on trust, it is essential to analyse risks, including legal risks, in order to be able to decide the required level of trust. As indicated in the Preliminary Conceptual Models for the TrustCoM framework[5], trust is related to risk in two ways:

---

[4] Camarinha-Matos, L., Afsarmanesh, H., Löh, H., Sturm, F., Ollus, M. A strategic roadmap for advanced virtual organizations. In Collaborative networked oganizations: a research agenda for emerging business models. Camarinha-Matos, L and Afsarmanesh, ed. New York: Springer 2004, p. 296

[5] TrustCoM ID 1.1.2, V 1.0, p. 25.

(i) Risk Driving Trust: In this view the level of risk determines the necessary level of required trustworthiness, i.e. risk drives the decision making.

(ii) Trust Driving Risk: In this perspective we protect ourselves by only collaborating with principals that are likely to be well-behaved and as a result an interaction with them is not very risky.

This is also relevant in our context: If there is a high level of risk (including legal risk), then this requires a high level of trust. An example of this relation between risk, trust and legal protection can be found in the analysis of the TrustCoM collaborative engineering scenario (Appendix A).

2.2.3 Legal Risk Management

For the purpose of this study we understand legal risk management as a set of coordinated activities to direct and control an organisation, a relation between organisations or a system with regard to legal risks. The system could both be an information system or a set of contractual rules – or even the integration of contractual rules with policies in a VO information system. The term legal risk is here understood rather widely to include both risks that can *affect legal rights* and risks that can be *treated by "legal treatments"*, in particular contracts. The term risk is defined in the ISO vocabulary for risk management as the combination of the probability of an unwanted event and its consequences.[6]

In a legal risk analysis, forming a part of the legal risk management, we should include both normative and non-normative unwanted incidents. An unwanted incident can be understood as normative, if the incident is prescribed as a consequence of one or more legal rules. A simple example: A company may be fined according to Section 47 of the Norwegian Data Protection Act, as a consequence of specific breaches of the Data Protection Act. As the example illustrates, the analysis of normative unwanted incidents is related to the question of compliance with existing legal rules. This is an obvious interface to the classical legal methods, and these can be used to assess whether the organisation or system is compliant with applicable rules. However, while legal methods are valuable for assessing compliance, they afford little guidance with respect to the proactive identification of facts that need to be assessed. Here, risk analysis methods can be useful as complementary methods to support the identification of normative unwanted incidents.

An unwanted incident lacks normative character if the incident is not a consequence of a legal rule. As an example, consider that a particular piece of business information is communicated to a competitor, who could use the information for competitive purposes. The consequent loss of market share of the stakeholder of the information is in itself not a consequence of a legal rule, but a fact related to economic mechanisms. Nevertheless, the likelihood of the occurrence of this unwanted incident may be reduced to a certain extent through a confidentiality clause in a VO contract, i.e. a legal rule.

---

[6] ISO *Risk management - vocabulary - guidelines for use in standards* (Guide 73 2002), 3.1.1.

2.2.4 Legal Risk Analysis Related to VO Contracts

The establishment of a VO often occurs under the pressure of time in order to avoid losing the business opportunity, which is the primary driver for the collaboration. On the other hand, the parties need to define a contract that sets out the internal functioning of the VO; the contract is a key mechanism for the VO management.

In such cases it is advisory to base the contract on an existing template, which can be adapted to the needs of the VO. However, such contractual templates can not be used “off the shelf”; they need to be adapted to the needs of the specific VO. This implies an adjustment of the contractual rules, taking into account the specific aim of the collaboration, how the partners want to organize the internal management of the VO, if the VO structure is more static or more dynamic, and what kinds of specific risks have to be taken into account.

Legal risk analysis can be applied to the process of adjusting a contract template to the specific risks of the VO. The VO needs to avoid two situations: First, the contract should not overlook relevant risks that should have been addressed in the contract. Second, the contract should avoid addressing issues that are of little business relevance, since the contractual terms could themselves present a barrier for a successful collaboration, e.g. by providing very bureaucratic rules for cooperation.

When drafting a contractual rule, risk management has to consider both non-normative unwanted incidents – since these motivate certain contractual rules – and normative unwanted incidents. Both kinds of unwanted incidents can be identified at different levels: First, the *situation* to be regulated in the contract may generate unwanted incidents, e.g. it could lead to liability. Second, the contractual *rules* themselves may generate unwanted incidents, e.g. by establishing the possibility for contractual liabilities. Third, the *application of the rule* could cause unwanted incidents, e.g. because of an unclear contract clause.

2.2.5 Graphical language and formalisation of legal issues

In TrustCoM we have developed a graphical language tailored to modelling of legal risks, based on the CORAS graphical language for threat modelling.[7] This language is aimed at facilitating communication and understanding between all the different participants of the risk analysis, e.g. system developers, lawyers and decision makers, through the use of graphical models to document both the target of the analysis (e.g., the system, organisation or process being analysed) and the outcome of the analysis itself.

The CORAS language covers notions like asset, threat, risk and treatment, and supports communication among participants with different backgrounds through the definition of easy-to-understand icons (symbols) associated with the modeling elements of the language. We have extended the CORAS graphical language with

[7] Folker den Braber, Mass Soldal Lund, Ketil Stølen, Fredrik Vraalsen. The CORAS methodology: Model based security analysis using UML and UP. Encyclopedia of Information Science and Technology. Information Resources Management Association, USA (2005)

concepts related to legal issues, such as obligation, permission and ownership, which were identified as being relevant during the legal risk analyses of the TrustCoM scenarios.

The language needs to be easily understandable for practitioners and at the same time sufficiently precise to allow in-depth analysis. The objectives of this workpackage include "formalisation of legal issues, so tool support can be provided". We are defining a precise semantics, or meaning, for the language through the use of formal methods. Whereas the practitioners involved in legal risk analysis need not necessarily consult, or even grasp, the details regarding the formalisation of the language, the formalisation is nevertheless important for the development and use of the language, both for explaining the meaning of the graphical models to the users and to facilitate the development of automated tools for processing the graphical models.

The graphical language is an extension of the Unified Modelling Language (UML) 2.0 specification language,[8] the de facto standard modeling language for information systems. The choice of a UML based language for modelling of legal risks was also motivated by the use of UML as a basis for much of the technological development in the TrustCoM project.

The work related to the graphical language is described in more detail below in Section 7 and in Appendix D and E of this report.

2.3 Structure of the document

The remaining sections of this report are structured as follows:

- Section 3 describes the results of the legal risk analysis of the CE scenario with respect to intellectual property rights. These results are detailed in Appendix A of this main report.
- Section 4 includes the analysis of international issues (choice of law and jurisdiction), based on the AS / eLearning scenario, detailed in Appendix B.
- Section 5 refers the results of the analysis of legal issues related to data protection law, which are presented in more detail in Appendix C.
- Section 6 discusses legal requirements to trust, security and contract management.
- Section 7 regards the conceptual model and the graphical language for legal risk analysis, which are discussed in more detail in Appendices D and E.
- Section 8 presents our concluding remarks.
- Section 9 points to the Appendices of this report, which can be found in separate documents.

[8] OMG: UML 2.0 Superstructure Specification. OMG Document: ptc/2004-10-02.

3 INTELLECTUAL PROPERTY LAW

The following section provides a summary of some of the findings of the legal risk analysis carried out with respect to the TrustCoM Collaborative Engineering (CE) scenario. The complete risk analysis report is included in Appendix A.

3.1 Legal Risk Analysis in the CE Scenario

The goal of the analysis was twofold; 1) to identify legal risks and treatments related to intellectual property rights (IPR) in the selected VO scenario, with the aim to create a set of reusable results for use in future analyses, e.g. in the form of templates and checklists, and 2) to evaluate the suitability of risk analysis, in particular the CORAS model-based risk analysis (MBRA) methods and graphical language, with respect to supporting the analysis of legal issues in relation to contract formation in VOs.

We have performed the legal risk analysis on the basis of the TrustCoM CE scenario. In short, the scenario encompasses three VOs:

- An airliner VO, (Air VO) consisting of the carrier, support and maintenance teams;
- A Collaborative Engineering VO, (CE VO) which has the technical expertise to support the specification and integration of systems into complex products, and which may take the decision to manufacture the solution for the customer. This VO's business goal is to win a contract with the Air VO regarding the upgrade of a particular aircraft type with an in-flight entertainment system. One of the partners of the CE VO, the Systems Integrator (SI), is specialized in the integration of different aircraft systems.
- A number of engineering analysis consultancies that form a VO to support design activities within engineering companies. The Analysis VO (AVO) supports general analysis work across engineering and scientific sectors.

It can be assumed that a number of different contracts will govern the internal and external relations in the CE scenario. These will most probably include at least three types of contracts:

- Consortium agreements, which establish a consortium of organizations with a common goal. In the TrustCoM conceptual models, this type of contract is referred to as General VO Agreements (GVOA).
- Services or goods related contracts, which govern the provision of services or the purchase of goods without establishing a consortium.
- Service Level Agreements (SLAs), i.e. more specific (electronic) contracts that deal with the specific rules that partners in an operational business process are bound to. These can be included in, or related to, both consortium agreements and services related contracts.

3.2 Intellectual Property Rights and Confidentiality

The scenario will include at least the following types of contracts: (1) VO-internal consortium agreements, encompassing all CE VO members. (2) Service or goods related contracts and/or SLAs, between the CE VO (possibly represented by a lead contractor) and the two other VOs, AVO and Air VO. Both types of contracts should also cover IPR issues.

Intellectual and industrial property rights consist of a variety of rights, including copyright, database protection, patent protection, trademark and design protection and the protection of confidential information (i.e. know-how and trade secrets). The legal framework for these rights differs to a certain extent, taking into account the nature of the protected right. Intellectual property law is regulated slightly differently in member states of the European Union despite a harmonization of selected IPR issues in European law.

For a VO, the protection of copyrights is closely related to the question of legal personality. In principle, only an entity with legal personality can hold legal rights. Therefore, if the VO has legal personality, it can hold most intellectual property rights. VOs that lack legal personality must refer to their members as holders of all legal rights. A general analysis of IPR issues in a VO context was carried out by the ALIVE project.[9]

Relevant IPR issues that are likely to be encountered in the formation and operation of a VO can, for the sake of simplicity, be split into two principal categories: Internal issues arise among the various members of a VO, whereas external issues arise between the VO and/or its members, on the one hand, and parties outside the VO on the other hand. We should also make a distinction between pre-existing IPR, which is brought into the VO by the partners, and the IPR developed during the co-operative process.

With respect to the CE scenario, the most important issue is the protection of confidentiality in relation to trade secrets and other business confidential information. Whilst our main focus is the protection of IPR in a contractual context, we also attempt to relate the legal issues to the trust and security issues addressed in other parts of the TrustCoM project.

3.3 Selected Results of the Legal Risk Analysis

This section presents selected results of the legal risk analysis, which was performed according to the CORAS risk analysis process. The initial step of this process consists of describing the context of the analysis, i.e. the target of analysis and relevant stakeholders and assets. The target of evaluation for the risk analysis was the scenario presented in Section 3.1, with a focus on the analysis of IPR, as detailed in Section 3.2, in particular know-how and trade secrets (confidential information). The analysis was performed from the viewpoint of the airplane Systems Integrator (SI) partner of the CE.

[9] ALIVE IST Project, *Report D 13, Intellectual & Industrial Property Rights*. http://www.vive-ig.net/projects/alive/docs.html.

The risk identification was performed during a number of HazOp brainstorming sessions involving participants from WPs 6, 8 and 9 with backgrounds in law, economics, computer science and philosophy. Risks were assigned consequence and frequency values and prioritised, and treatments were then identified for the major risks through another brainstorming session. Some examples of identified risks and treatments are presented below. For a more comprehensive analysis, please refer to Appendix A.

3.3.1 Example of Identified Risks

The identified risks relate to different IPR issues, including the protection of confidential information (i.e. know-how and trade secrets), the ownership of IPR, and liability for IPR infringements by other VO partners. It would be outside the scope of this main report to present all identified risks, they are included in Appendix A. We will here concentrate on risks related to the loss of confidential information, which was identified as a major risk category. The internal collaboration in the CE VO and its cooperation with the AVO and the Air VO, respectively, may imply that confidential information is shared or otherwise disclosed to VO partners or to other VOs. This involves a risk that such confidential information is disclosed to third parties, or used by VO members for purposes that are not related to the VO.

Figure 1 shows a CORAS UML diagram describing some ways in which confidential information can be disclosed and potential consequences this disclosure may have. In the CORAS language for risk analysis, a threat is described using a *threat agent*, e.g. a disloyal employee or a computer virus, typically represented in the diagram by a stick figure. The threat agent initiates a *threat scenario*, which is a sequence of events or activities leading to an *unwanted incident*, i.e. an event resulting in a reduction in the value of the target *asset*. Furthermore, an unwanted incident may initiate or lead to another unwanted incident, forming a chain of events. For example, an unfaithful employee working for one of the CE VO partners may have access to confidential information, which he/she could disclose to a third party. This disclosure could lead to the information reaching the public domain and thereby losing its legal protection and value as a trade secret. A similar but opposite scenario is that an employee of our stakeholder (SI) is unfaithful and discloses the client's confidential information. This again could lead to the CE VO or the SI being sued for breach of the non-disclosure agreement with the Air VO. The latter unwanted incident may not only have consequences for the SI's revenue, it may also lead to further consequences, like negative publicity.

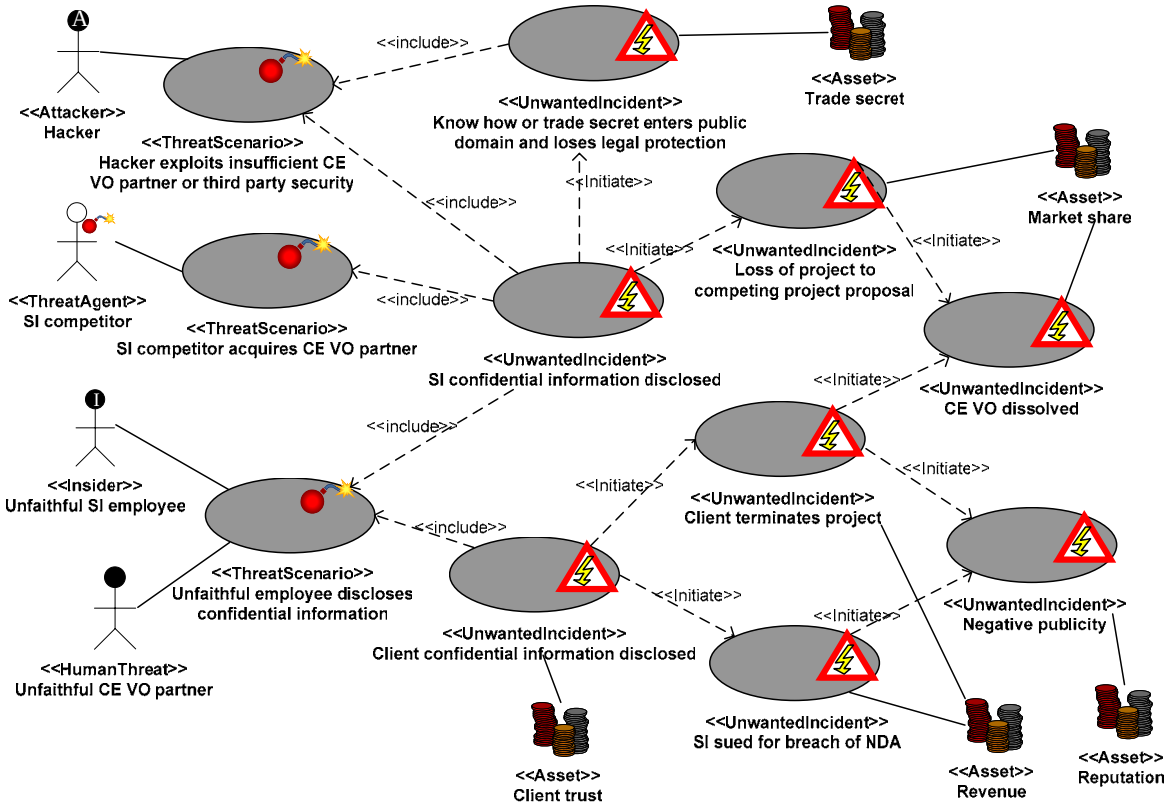

Figure 1 Confidential information loses legal protection

3.3.2 Example of Identified Treatments

For each of the risks, we have explored potential treatments related to three main areas of the TrustCoM project, namely trust, security and contracts. Our aim was to develop an integrated set of treatments, where legal and other measures interrelate. In this context we focused on law as a proactive mechanism, which tries to solve legal issues before they arise; legal reactions *ex post* were not addressed.

Treatments may have different effects on risks, they may e.g. reduce the consequence or frequency of the unwanted incident occurring, or transfer the risk to another party, e.g. through insurance. A selection of treatments to the risks described above is shown in the CORAS treatment diagram in Figure 1. Two of these treatments are clearly within the legal domain: First, a contract clause could avoid the disclosure of confidential information in case of a merger or acquisition, by allowing a re-negotiation of the general VO agreement in this event. Second, specific contractual rules in the VO agreement should address the VO members' liability towards third parties. The remaining treatments involve legal and non-legal elements: Information security mechanisms like limitations to storage time and the deletion of data after an analysis are of key importance. Such mechanisms can be made obligatory via contractual clauses in the agreement between the CE VO and the AVO. If the technology was available, a VO-internal enterprise Digital Rights Management System (DRM) could also reduce the likelihood of confidential information being disclosed, particularly if some of the contractual obligations could be enforced through technology.

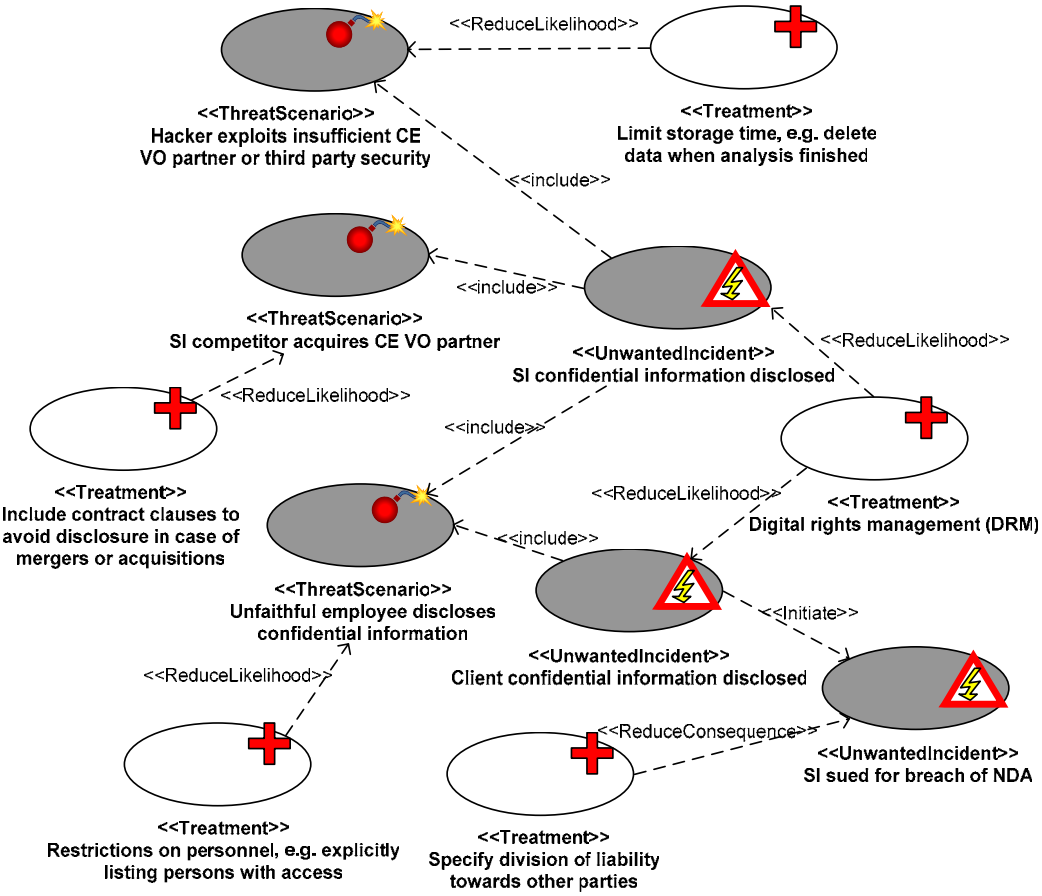

Figure 2 Risk treatments

3.4 Concluding Remarks for Section 3

We have presented results from the analysis of the collaborative engineering scenario, where a number of legal risks and treatments were identified. Our risk analysis results indicate how legal risks, such as the loss of protection of confidential information, can be treated by an integrated solution, including contractual elements, trust management and security management. Interestingly, many of the relevant contractual treatments were also included in a general manner in the ALIVE contract template for VOs.[10] The performed legal risk analysis provided indications about how these rules can be adapted to the specific scenario. Since the graphical representation implies a simplification, a lawyer would have to integrate analysis results into the contractual document in an appropriate way, taking into account the terminology and the system of the contractual template.

The analysis results were generated during a number of brainstorming sessions involving participants from WPs 6, 8 and 9 with varied backgrounds, including law,

[10] ALIVE IST Project. Report D 17 a, VE Model Contracts, available at http://www.vive-ig.net/projects/alive/docs.html.

informatics, economics and philosophy. Based on our experiences, the graphical models can indeed facilitate the communication and understanding with respect to legal issues in a multidisciplinary context.

4 INTERNATIONAL ISSUES

This section describes the research performed with respect to the TrustCoM AS scenario, which was analysed with a focus on international issues, i.e. jurisdiction and choice of law in relation to VOs. The detailed results of this work are presented in Appendix B.

In this study we have (i) discussed and clarified some of the contractual relations between the different VO partners in the TrustCoM AS (E-Learning) scenario and (ii) analysed legal risks relating to private international law with respect to this scenario.

In short, the scenario describes an Enterprise Network (EN) that offers aggregated E-Learning services. One or more Training Consultants (TCs) provide an interested learner with learning paths, consisting of a number of learning resources offered by Learning Content Providers (LCPs). The involved TCs and LCPs form a new VO for each learning path they provide in order to administrate the specifics of this learning path.

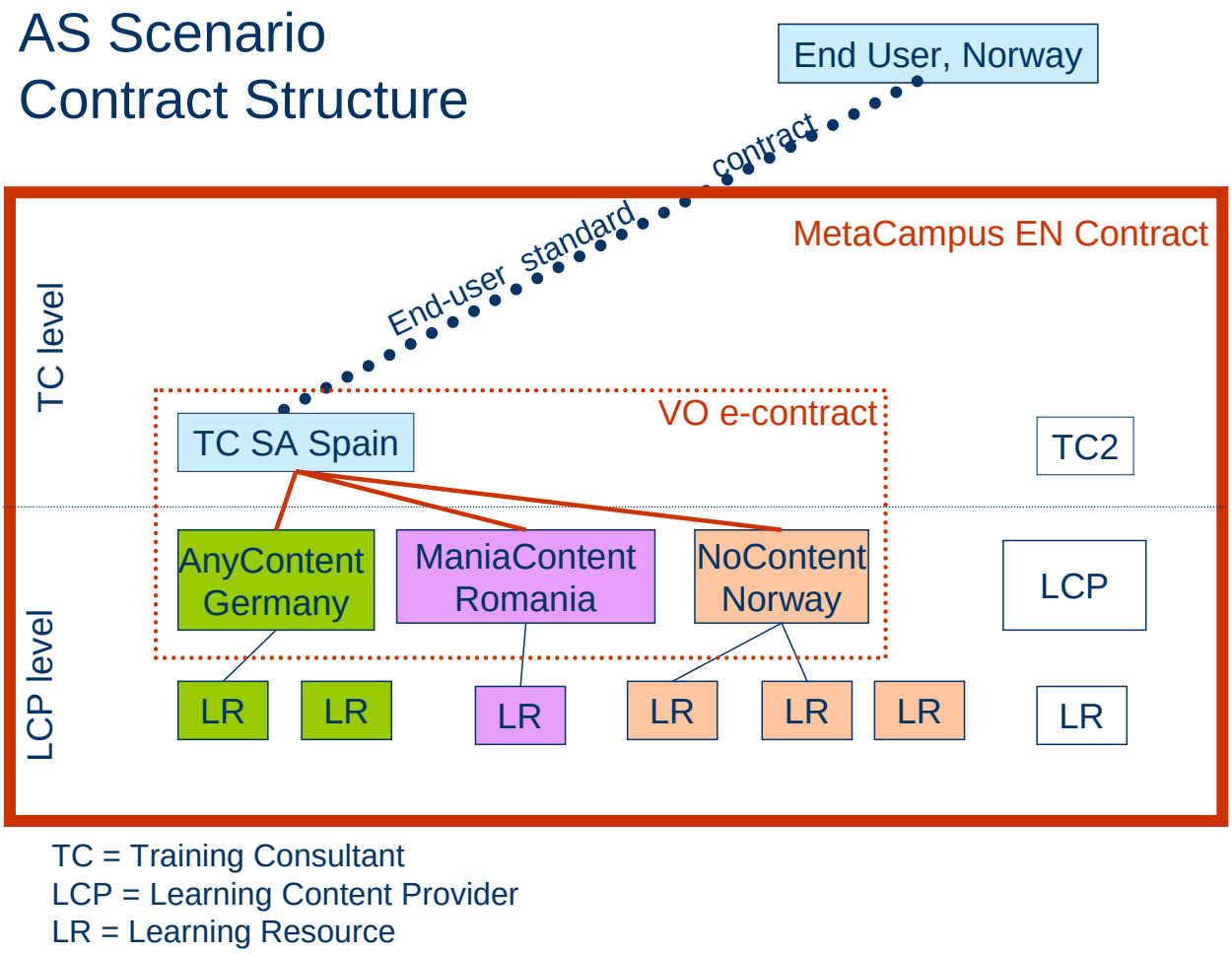

Figure 3: A possible contract structure for the AS scenario, illustrating the cross-border relations of VO participants and customers

A number of contracts should be put in place for the scenario to be operable: First, the EN should regulate the general co-operation among all EN members. Second, for those involved in a specific co-operation, there should be an internal contract defining how the aggregated services will be performed. The third contract level will be an end-user contract. The latter could either be concluded by only one VO member in its own name, or it could involve all VO members, e.g. represented by one VO member who acts as an agent. This description of contractual relations was used as a basis for the legal risk analysis, which focused on choice of law and jurisdiction.

From a risk analysis point of view, a discussion limited to choice of law and jurisdiction enables us to identify relatively few unwanted incidents, e.g. the possibility of being subjected to a costly lawsuit in a foreign country, or the risk of a less favourable decision based on an applicable foreign law. The majority of (normative) unwanted incidents can not be found in the body of law regulating choice of law and jurisdiction, but rather in the material law that regulates e.g. liability issues. However, addressing issues related to jurisdiction and choice of law in a risk analysis is necessary to determine where to find further normative unwanted incidents. Hence, discussions of choice of law and jurisdiction are useful in a legal risk analysis context, both to identify and highlight the unwanted incidents that directly relate to this body of law, and to provide the necessary step towards the body of law that may concern further details about possible unwanted incidents.

Most of the identified legal risks related to choice of law and jurisdiction can be managed by a VO: First, for the internal relations of the VO members, the general agreement establishing the VO or the Enterprise Network should contain clauses defining that all internal contracts and relations exclusively be governed by one law and one jurisdiction. Save for matters relating to tort, delict and quasi-delict, this should effectively reduce the insecurity in VO-internal matters. Second, for the external relations of the VO, jurisdiction and choice of law can only be chosen freely if the contract partner is not a consumer. If however the contract is or may be concluded with a consumer, then the choice of law and jurisdiction is limited as described in Appendix B. If a VO wishes to further reduce the applicability of foreign laws and the competence of foreign courts, it may utilize some of the mechanisms discussed in Appendix B, Section 5.

5 DATA PROTECTION LAW AND REPUTATION SYSTEMS

This section presents selected elements from the study of reputation systems in relation to data protection law. This study, presented in Appendix C, was carried out on the basis of a virtual community scenario, where personal information is processed in a reputation system. Reputation systems play an important role in TrustCoM, as a means to ensure trust.

Reputation systems collect information about a person or other entity (hereinafter "reputation subject") in order to evaluate the reputation subject's conduct and make this evaluation accessible for other users' decisions. An example is when Internet marketplaces like eBay* and Amazon.com* enable users to provide feedback on other users. In this case, feedback ratings are based on a user's past transactions and help other users learn about the transaction partner they are dealing with. Other examples include credit reporting services, which collect information about an entity's economic behaviour. This information is communicated e.g. to banks when they decide about credit. The latter kind of reputation systems has existed for a long time, but recent developments with respect to Internet based transactions have led to an increased need for reputation systems.

Reputation systems may be of particular value when there is uncertainty about another person or entity involved in a planned transaction that involves risk. Transactions on the Internet involve a number of uncertainties with regard to the identity of the transaction partner, his or her ability and willingness to perform, and the availability of realistic means of enforcement. The lack of experience, knowledge or information about the other person or entity may lead us to refrain from the interaction. Reputation systems can provide us with relevant experiences others have had with this person or entity. Research indicates that reputation systems can encourage market actors to participate in transactions.[11] Reputation systems have also been considered as a compensation or supplement for lacking realistic means of enforcement on the Internet.[12, 13, 14]

Reputation systems should be carefully designed in order to comply with data protection law, if they (at least in part) deal with personal data. This will ensure a

---

* Trademarks or registered trademarks of eBay Inc. and Amazon.com Inc.

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

[12] Friedman, D., Contracts in Cyberspace, available at http://www.daviddfriedman.com/Academic/contracts_in_%20cyberspace/contracts_in_cyberspace.htm, last visited 23 April 2004.

[13] Gilette, C.P., Reputation and Intermediaries in Electronic Commerce, Louisiana Law Review, Summer 2002, pp. 1165–1197.

[14] Block-Lieb, S., E-Reputation: Building Trust in Electronic Commerce, Louisiana Law Review, Summer 2002, pp. 1199–1219.

fair administration of information, and users will more easily accept to participate in the reputation system. The basic data protection principles can also be considered as a means to improve the data quality in a reputation system, which makes the reputation system more relevant as a basis for a decision and more attractive for the end-user. Below, we have tried to capture some relevant factors that should be considered to ensure that reputation systems respect data protection law.

- Participation in a reputation system should be limited to actors who have expressed their well-informed consent.
- The purpose(s) of the reputation system should be clearly defined.
- The collection, storage and dissemination of (personal) data should be limited to the amount necessary to achieve the purpose(s).
- The procedures regarding the collection and evaluation of personal data should be transparent and communicated in a comprehensible way.
- Reputation subjects should be allowed some participation and control with respect to the collection of data about them and with regard to the generation of their reputation profile.
- The quality of both the collected data and of the aggregated reputation profile should be valid with respect to what they are intended to describe and relevant and not incomplete with respect to the specified purpose(s).
- Fully automated decisions on the basis of reputation profiles should be avoided. If they are chosen, there should be full transparency regarding the algorithms used to calculate the reputation score and to make the decision. Additionally, the data subject should be able to claim a human decision.
- The security of (personal) data must be ensured.
- Reputation systems that deal with sensitive data should use a stricter policy to protect personal data.

These recommendations may assist in identifying legal problems, indicating that the reputation system developer and the data controller should seek legal advice to clarify how the law in the relevant jurisdiction solves these issues.

6 LEGAL REQUIREMENTS FOR TRUST, SECURITY AND CONTRACT MANAGEMENT

The following sub-sections provide some legal requirements for trust, security and contract management with respect to VOs. The requirements are primarily based on the findings of the legal risk analyses carried out with respect to the CE and AS scenario. In addition, we refer legal requirements, which have not been analysed in our studies, but which are or may be of relevance for trust management, security management or contract management of virtual organisations. We have attempted to extract some key legal factors that either require a particular mechanism or that set out restrictions with respect to trust, security and contract management. These requirements describe selected aspects of the legal context for the TrustCoM framework, but they are not meant to be exhaustive.

6.1 Trust Management

This section attempts to point out some legal requirements to trust management. We understand trust management in the sense this term is used in TrustCoM ID 1.1.2, Section 5: “The overarching aim of Trust Management in the TrustCoM project is the development of an integrated model of trust which will enable (potentially) participating members of a VO to retrieve, record and manipulate measures of trust and reputation in other (potentially) participating members over a range of methods for the evaluation of such measures.”

There are two ways how laws can provide requirements for trust management: First, trust management can be useful to minimize legal risks. Second, the use of trust management may be limited by laws.

6.1.1 Trust Management as a Means to Reduce Legal Risks

Trust management is indeed important also from a legal point of view. For example, trust is a key issue for a prospective VO participant who wants to protect confidential information (trade secrets and know-how). In this context it is important to ensure that the other VO partners are sufficiently trustworthy to be entrusted with confidential information. The trustworthiness of cooperation partners is one of the issues that are addressed in a due diligence procedure commonly carried out prior to entering into a joint venture agreement.[15] Appendix A, Section 5.1 discusses in more detail how trust management can reduce the risk of losing confidential information with respect to the TrustCoM CE scenario.

[15] See details in S Sayer *Negotiating international joint venture agreements* (Sweet & Maxwell London 1999), part one chapter 3.

6.1.2 Legal Limitations to Trust Management

The utilization of trust management may in some cases come in conflict with legal rules. In this sense, laws may limit the possibility to use trust management. However, it is difficult to define legal limitations for trust management in the abstract. Legal rules are always related to a specific context; outside this context the rule is inapplicable. The following sections will focus (i) on the contractual context, (ii) on the protection of personal data, and (iii) on the legal protection against defamation.

6.1.3 Contract Law

From a contractual perspective there is a major difference between trust management prior to entering into a contract, and trust management once a general VO agreement is established. Once the contract is a fact, any type of trust management (e.g. reducing access rights of a VO partner who is no longer considered as completely trustworthy) has to be backed up by the GVOA or applicable law. This is contrary to the pre-contractual phase, where the parties in principle[16] are free to decide if they want to enter into a contract, who should be the contractor, and what should be the content of the contract. Consequently, there is a much greater freedom to apply trust management measures during the pre-contractual phase (VO identification and formation), compared to the contractual phase (VO operation and dissolution).

Legal requirements to contract management are discussed below in Section 6.3.

6.1.4 Data Protection

Trust information may be personal data, which only can be processed under the conditions laid down in data protection laws. For a more detailed analysis of this issue please refer to Appendix C.

6.1.5 Defamation

Under some particular circumstances trust and reputation related information may qualify as defamation, which is criminalized in most countries. It is outside of the scope of this report to go into any details on this. According to the Black's Law Dictionary, defamation covers the following actions: "Holding up a person to ridicule, scorn or contempt in a respectable and considerable part of the community […] A communication is defamatory if it tends to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him. The meaning of a communication is that which the recipient correctly, or mistakenly but reasonably understands that it was intended to express". Note that defamation may have consequences both with respect to

[16] Note however that many laws foresee pre-contractual duties, based on good faith and fair dealing. Moreover, a number of pre-contractual notes and preliminary contracts may be in place to rule this phase. For a more detailed description of this phase see ALIVE IST Project *VE Model Contracts, Deliverable D 17a* (2002).

criminal law and with respect to private law. Different jurisdictions have diverse rules with respect to what is criminalized as defamatory. In particular, defamation laws have to be understood in the context of freedom of speech, which may override the prohibition of defamation. Note also that defamation according to some jurisdictions is only applicable with respect to individuals, while corporate entities or organisations are not deemed to have a reputation that requires the same level of protection.

Hence, defamation legislation may be seen as a limiting factor for trust management in some extreme cases. Therefore, it is important to include measures to ensure fairness in a trust management system. It may be the case that some of the measures included in Appendix C (regarding measures to ensure privacy and data protection) also can assist in ensuring fairness in the context of defamatory statements.

6.2 Security Management

Information security is an important issue from a legal perspective. A number of laws require measures to ensure information security. Again the legal requirements depend on the context, e.g. the protection of personal data or the protection of commercially sensitive information including trade secrets or know-how.

6.2.1 Data Protection

Data protection laws in Europe require that information security measures are in place to protect personal data. The basis for these rules is Article 17 of the EC Data Protection Directive, which reads as follows:

> "Article 17 Security of processing
>
> § 1 Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
>
> Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.
>
> § 2 The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.
>
> § 3 The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:
>
> - the processor shall act only on instructions from the controller,
> - the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

§ 4 For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form."

Hence, if personal data is processed in relation to the operation of the VO, the above rule should be considered as a legal requirement. Data protection issues may be of importance to the AS scenario, since it may involve the processing of personal information about the customers of the e-learning service.

6.2.2 Protection of Business-Related Confidential Information

Security management plays an important role with respect to the protection of confidential information and trade secrets from misappropriation and disclosure. From a legal point of view, the TrustCoM framework should ensure that adequate security measures are in place, that effectively reduce the likelihood of confidential information or trade secrets either being disclosed to third parties (including competitors and the public) or being misappropriated in the sense that the information is used by a VO partner in a way incompatible with the VO contract. This is discussed in more detail in Appendix A, Section 5.2.

6.3 Contract Management

Contracts play a key role as a mechanism to administrate the internal relations between the VO members and as an instrument to govern the external relations with customers and third parties. In general, laws contain a number of formal and material requirements for contracts. This section cannot provide a comprehensive list of all the legal requirements for contracts and contract management; it merely illustrates how some legal requirements will affect some of the VO-related contracts.

As a rule, a contract is formed as soon as the offer made by one entity (for example, the Training Consultant) is accepted by the recipient (the natural or legal person to whom the offer was addressed, e.g. a certain LRP) and the intention to be bound by the contract is communicated. The way in which the parties externally manifest their willingness to be bound by a contract (written form, orally in the presence of witnesses, electronic contract, even through an audio recording) represents "the form" of the contract. Note that the term formal in this Section (as opposed to e.g. Section 7) is meant to be used with a legal meaning.

Since contracts are consensual acts, the law generally imposes few requirements regarding how the contract should "look like" in order to be recognized as valid, as long as the parties agree to the contract's key terms. However, even though there may be no requirements regarding the form of a particular contract, the form chosen by the parties will nevertheless influence the easiness of proving both the fact that it was adopted, as well as its contents. In other words, the existence of a "form-free contract" may be recognized by law, but may in practice be more or less difficult to prove in a court that the contract was concluded and what the parties agreed to.

There are however certain contract types, e.g. related to real estate property or to specific transactions regarding corporations, for which a particular form is prescribed. In these exceptional circumstances, specified exhaustively in national laws, the law will not recognize the contract as valid, unless the will of the party to be bound by a contract is embedded in a certain form (for example in writing in front of a public notary). In this case, the contract will be legally considered as inexistent, even though parties or witnesses could show that an understanding was reached. This will, for example, regularly be the case when VO members want to create a new legal entity.

6.3.1 Contracts for virtual organisations

The required contractual framework for a VO will essentially depend on many factors, including:

- the specific aim of the collaboration (the business objective),
- the duration of the collaboration,
- the number of participants,
- how the partners want to organize the internal management of the VO,
- whether the VO structure is more static or more dynamic,
- and specific risks related to e.g. the protection of intellectual property.

An example template for a VO contract has been produced by the ALIVE IST project.[17] As illustrated by the AS scenario discussed in Appendix B, a VO may also have a relation to an EN, and in this case it is advisable to regulate some internal issues in an EN contract. Such a contract could, for example, be based on the template for SME clusters, developed by the Legal-IST project.[18]

6.3.2 Cross-border contracts

As mentioned above in Section 4 and as further detailed in Appendix B, the international nature of many VO-related contracts needs to be taken into account.

6.3.3 E-Commerce Directive

Further requirements for contracts are defined e.g. in the E-Commerce Directive. [19] All information society service providers need to comply with requirements for contracts defined in national laws based on this directive. The term information society services covers any service normally provided for remuneration, at a

[17] ALIVE IST project, ibid, above fn. 16.

[18] See Appendix C of Report on Legal Issues in SME Clusters, to be published by the Legal-IST project, IST-2-004252-SSA, www.legal-ist.org.

[19] DIRECTIVE 2000/31/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce), Official Journal of the European Communities L 178/1-16.

distance, by electronic means and at the individual request of a recipient of services, which is defined in more detail in Directive 98/48/EC:[20]

- "At a distance" means that the service is provided without the parties being simultaneously present. This will usually be the case in the VOs targeted by TrustCoM.
- "by electronic means" signifies that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means,
- "at the individual request of a recipient of services" means that the service is provided through the transmission of data on individual request.

Article 9 of the E-Commerce Directive ensures that contracts, like contracts entered into by a VO, in principle can be concluded by electronic means. However, to the degree VO members provide services (like the service provided by the Training Consultant in the E-Learning scenario or analysis services in the CE scenario), they will need to comply with the duties laid down in the Directive.

According to Article 5 of the E-Commerce Directive, the service provider shall in particular render easily, directly and permanently accessible to the recipients of the service and competent authorities, at least the following information: (a) the name of the service provider; (b) the geographic address at which the service provider is established; (c) the details of the service provider, including his electronic mail address; (d) where the service provider is registered in a trade or similar public register, the trade register in which the service provider is entered and his registration number, or equivalent means of identification in that register.

According to E-Commerce Directive Article 10, the information to be provided in relation to contracts – at least when contracting with consumers – shall include, among other information, the technical steps to conclude the contract, information about storage an accessibility of the contract and about means for identifying and correcting errors when placing an order. Once an order has been placed, this has to be confirmed by the service provider according to Article 11.

6.3.4 Electronic signatures and evidence

Further legal requirements to contracts relate to the use of electronic signatures. The relevant EC Directive[21] differentiates in Article 2 between "electronic signatures" and "advanced electronic signatures". An "advanced electronic signature" is an electronic signature which meets the following requirements: (a) it

[20] DIRECTIVE 98/48/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 July 1998 amending Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations, Official Journal of the European Communities, L 217/18 et seq.

[21] DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures, Official Journal of the European Communities, L 13/12-20.

is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control; and (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable. Article 5 of the Directive lays down the circumstances in which electronic signatures are to be considered valid, enforceable and legally effective: For simple electronic signatures, the EU member states must ensure that signatures of this type are not denied validity, enforceability and effectiveness solely on the grounds that they are in electronic form and not certified. Regarding advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device, EU member states must ensure that these satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and that they are admissible as evidence in legal proceedings. However, for most transactions no handwritten signature is required and consequently, an advanced electronic signature is not a formal requirement for typical contracts between VO members and third parties, as illustrated in the TrustCoM scenarios.

It may be the case that some transactions must be entered into in writing or proved by a written act, which will depend on the requirements specified in national laws. Many jurisdictions have updated the requirements for the written form, thereby clarifying whether the written form also covers the electronic form.[22] However, the evidential weight of an electronic registry may be evaluated on a case-to case basis, once the question arises before a court.[23]

6.3.5 Consumer protection law

To the degree VOs contract with consumers, legal requirements will also follow from applicable consumer protection law, including those based on the Distance Selling Directive[24], which specifies the rights of the consumers who buy goods and services at a distance throughout Europe. Among the fundamental legal rights of the consumers in these circumstances, are:

- Provision of comprehensive information prior to the contract.
- Confirmation of that information within a durable medium (such as in writing).
- Consumer's right to withdraw from the contract within 7 working days.
- Contract performed within 30 days from the day after the consumer's order.
- A consumer cannot contract-out or waiver his rights provided under the directive.

---

[22] E.g. UK Electronic Communications Act 2000 s 8 (1) and (2) (a); US Federal Electronic Signatures in Global and National Commerce Act 2000, Section 301 (a); US Federal Rules of Evidence, rule 1001; Singapore Electronic Transactions Act 1998, Section 7.

[23] C Reed *Internet law: text and materials* (2nd edition Cambridge University Press Cambridge 2004).

[24] DIRECTIVE 97/7/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 20 May 1997 on the protection of consumers in respect of distance contracts, OJ L 144, 4.6.1997, p. 19.

The Directive also allows for the introduction or maintenance of further national rules to create a higher level of consumer protection.

It should be noted that a new Directive regarding unfair terms in business to consumer contracts was passed on 11 of May 2005[25]. The Member States have to transpose its provisions into national laws by 12 June 2007. Once implemented, these requirements will have to be taken into account by businesses especially when advertising services. The Directive also contains an Annex specifying which commercial practices will always be considered "unfair" when dealing with a consumer, as well as when dealing with a professional party.

[25] DIRECTIVE 2005/29/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), Official Journal 149/22, 11.06.2005

7 CONCEPTUAL MODEL AND USER-LEVEL LANGUAGE FOR LEGAL RISK ANALYSIS

As experiences from the legal risk analysis work performed in WP9 have shown (see Appendices A and B in this deliverable), we are able to use the existing CORAS graphical language for security risk analysis to document and analyse some aspects of legal risks, and the current language seems to be a good starting point for legal risk analysis. However, we wish to be able to model and analyse additional legal aspects, for example whether the act of accessing or distributing certain information, as illustrated in Figure 4, is forbidden by contract, e.g. by a non-disclosure agreement.

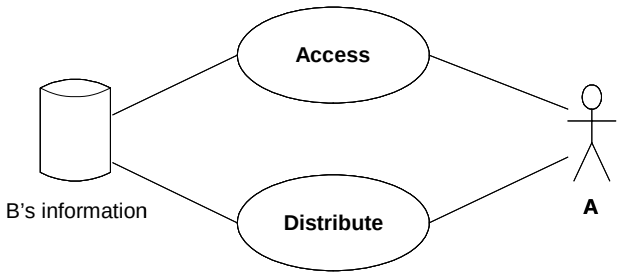

Figure 4 Activities relevant to confidential information

To enable this, we need facilities for:

- specifying normative positions like ownership or rights-holder, which are highly relevant when determining e.g. the rights and obligations of an actor,
- specifying legal effects on different roles and activities, and
- correlating these effects with the relevant legal sources, e.g. which contract clause is the source of the legal effect in question.

In legal risk analysis, parts of the target description will relate to legal rules formulated in legal texts such as laws and contracts. This motivates that target descriptions not only cover technical and organizational issues but also the legal issues. Legal texts have a tendency to be complex and also hard to read by laymen. Since participants of legal risk analyses will include people that are not legal experts, we claim that standard modelling techniques can be applied to give these participants a better grip of the legal issues.

We thus see the need to incorporate more information relevant to legal aspects into the graphical language. To facilitate the use of the graphical modelling language for documentation and communication of legal risk analysis results, the users of the language need a clear understanding of what the graphical models express. Furthermore, to support automated analysis of the graphical models, tools must be able to extract and process relevant information. To enable this, the concepts, as

well as the syntax and the semantics of the graphical language need to be defined, with particular emphasis on the notions of trust, security, privacy, data protection and intellectual property rights.

The goal is to develop a language that is (1) expressive enough to model concepts and relationships relevant to legal analysis and (2) easily understandable for practitioners and at the same time sufficiently precise to allow in-depth analysis.

With respect to (1), we are extending the existing CORAS graphical language with concepts and relationships relevant to legal analysis. These concepts and their relationships are defined by a conceptual model for legal risk analysis, which is presented in Appendix D. A central conjecture is that modal logic, in particular deontic logic, may be an important source of inspiration with respect to the kind of language constructs required. These enable us to specify which activities are permitted, obligatory or forbidden.

With respect to (2), we aim at giving a precise semantics, or meaning, to the extended graphical language by mapping it onto a logical framework. To facilitate the use of the graphical language for documentation and communication of legal risk analysis results, the users of the language need a clear understanding of what the graphical models express. Thus, we must be able to explain the meaning of the diagrams as well as how they can be combined and refined. Furthermore, a precise semantics is also a prerequisite for developing automated tools for processing the graphical models.

A preliminary version of the proposed language is presented in detail in Appendix E. This appendix falls into three main sections: requirements, abstract syntax, and concrete syntax:

- The requirements of the language are based on the experiences from the legal risk analyses of the TrustCoM scenarios.
- The abstract syntax defines the elements of the language. The conceptual model defined in Appendix D forms the basis for the abstract syntax of the language. Formalisation of this conceptual model in traditional first-order logic provides a tool for eliminating potential inconsistencies in the model, and can help reduce the complexity of the model by showing that a given relation is in fact an implicit consequence of those already in the diagram.
- The concrete syntax defines the graphical appearance of the elements of the language (e.g., icons in the UML terminology). We here show how to extend the CORAS graphical language with the concepts relevant to legal analysis.

The Consortium Agreement template for use by an SME cluster[26] provides suitable examples for illustrating some of the novel features of the language. According to paragraph 8.3.1(a), a member of an SME cluster is prevented from using any confidential information disclosed by another member of the cluster, except when the use is in accordance with an agreement. Figure 5 below shows how the language captures this situation.

[26] See Appendix C of Report on Legal Issues in SME Clusters, to be published by the Legal-IST project, IST-2-004252-SSA, www.legal-ist.org.

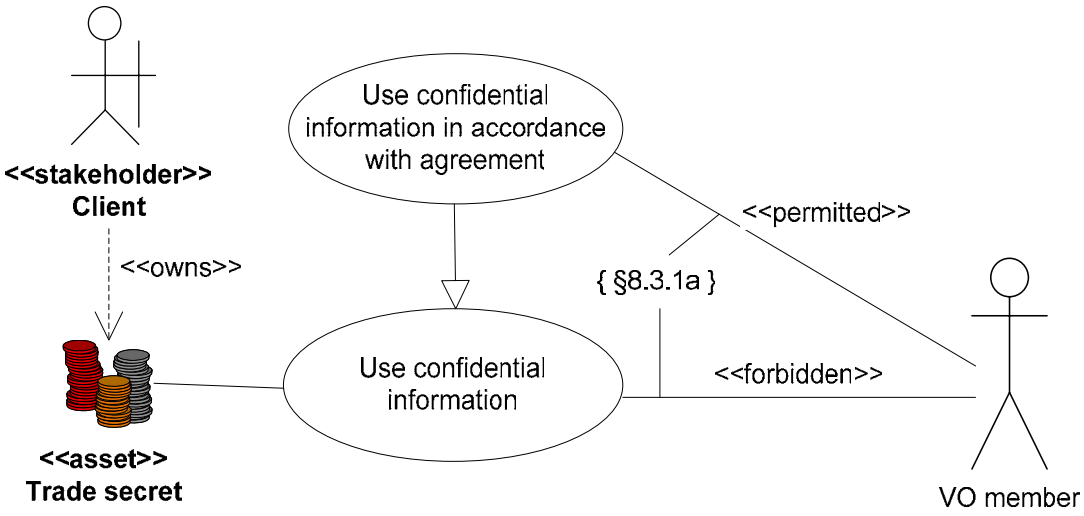

Figure 5 Obligations

Figure 5 illustrates several of the features of the language. First, the diagram specifies the "ownership", (more precisely, the position of the rights-holder) of the piece of information that is designated as confidential (i.e. the asset "trade secret"). Second, the rights and obligations of a given VO member, as specified by the agreement, are captured by relations between the VO member and the use cases. Third, the legal effects (permission and prohibition) are correlated with the legal source, i.e. paragraph 8.3.1a of the contract. Fourth, the diagram captures the allowance of exceptions from legal norms: According to paragraph 8.3.1(a), confidential information is generally not to be used by the VO member that receives this information; the information may, however, be used in case permission is granted by a specific agreement.

A further example from the Consortium Agreement template for SME clusters[27] illustrates how the language may capture legal aspects, in this case a contractual agreement, at different levels of granularity. According to paragraph 8.2, a disclosing member shall designate information as confidential at the time of disclosure. This is shown by the use case diagram at the left hand side of Figure 6 below. There is a pointer from the use case to an activity diagram which in detail outlines the procedure, as stated in the Consortium Agreement template, for designating information as confidential. This facility allows the users to carry out analyses at the appropriate level of granularity such that relevant information is expressed and irrelevant information is put aside.

The use of activity diagrams to illustrate the content of contract clauses is beneficial also by making the content of contract clauses intuitively understandable for practitioners and more accessible to non-lawyers.

[27] See Appendix C of Report on Legal Issues in SME Clusters, to be published by the Legal-IST project, IST-2-004252-SSA, www.legal-ist.org.

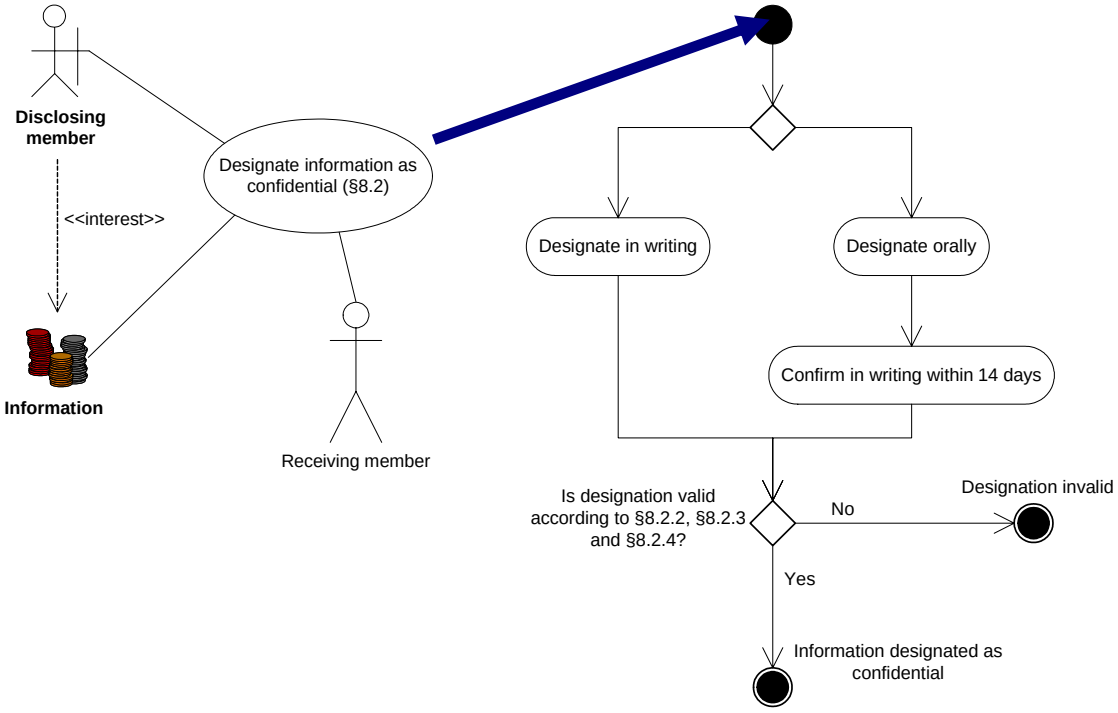

Figure 6 Designate information as confidential

Notice that generally UML, upon which CORAS is based, lacks a precisely defined semantics. In general the semantics of both UML and the CORAS language is described in English. For the purpose of adding the desired level of precision to the language for legal risk analysis, we aim at providing a formal semantics for our language constructs.

The formalisation of the language is based on the STAIRS semantics of UML sequence diagrams[28]. Sequence diagrams show the behaviour of objects in a use case, such as the ones in the figures above, in more detail. The details on the formalisation of the language can be found in Appendix E.

Whereas the practitioners involved in legal risk analysis need not necessarily consult, or even grasp, the details regarding the formalisation of the language, the formalisation is nevertheless important for the development and use of the language, both for explaining the meaning of the graphical models and to facilitate tool support.

Some elements of the concrete syntax still remain to be defined formally. For instance, it remains unclear how the ownership relation (see Figure 5) should be interpreted. This and other notions will be dealt with in future work within TrustCoM.

[28] See Ø. Haugen, K.E. Husa, R.K. Runde, K. Stølen, Why timed sequence diagrams require three-event semantics, *Post-proc. of Dagstuhl seminar, Scenarios: Models, Algorithms and Tools*, LNCS 3466, pages 1-25, Springer, 2005, and R.K. Runde, Ø. Haugen, K. Stølen, Refining UML interactions with explicit and implicit non-determinism, to appear in the *Nordic Journal of Computing*.

The developments presented in Appendix E aim ultimately to contribute to the overall TrustCoM project, by providing a bridge between the UML-based conceptual modelling done within AL1 and the legal issues part of the project. This is explained in more detail in Appendix E, Section 5.

8 CONCLUDING REMARKS

This report summarises the research performed in TrustCoM work package 9. The legal work contributes to the overall TrustCoM framework by defining some basic legal requirements for trust, security and contract management in VOs. Moreover, the study applies legal risk management to analyse legal issues related to trust, security and contracts in VOs. Since legal issues largely depend on the specific context, the nature of the collaboration and its purpose, the research mainly focuses on issues of relevance to the scenarios selected by the project.

With respect to the collaborative engineering scenario the legal risk analysis focuses on intellectual property rights and confidentiality. The risk analysis results indicate how legal risks, such as the loss of protection of confidential information, can be treated by an integrated solution, including contractual elements, trust management and security management. The contractual treatments should consist in an adaptation of a contract template to the specific risks identified in the scenario. The legal risk analysis provided some first indications about how a confidentiality clause can be adapted to the specific scenario. Since the graphical representation implies a simplification, a lawyer would have to integrate analysis results into the contractual document in an appropriate way, taking into account the terminology and the system of the contractual template. This indicates the need for a more detailed analysis of confidentiality clauses in VO contracts.

The legal analysis of the E-Learning scenario focused on legal risks related to international issues, i.e. choice of law and jurisdiction. While the international nature of a VO has few implications for the computational infrastructure of a VO, it is a factor of major importance in a legal context. However, most of the identified legal risks relating to international issues may be mitigated by defining an exclusive jurisdiction and an applicable national law in VO-related contracts. The remaining legal risks, particularly in relation to consumer contracts, should be tolerable and relate to the special protection for consumers. Future work in relation to the E-Learning scenario will focus more on the analysis of legal issues related to the access to digital content, and how the computational access may be integrated with the contractually agreed access.

The utilisation a UML-based graphical language in the legal risk analyses ensured compatibility of the legal study with other work in TrustCoM. The latter language was extended with legally relevant concepts, in order to make it more suitable for the analysis of legal issues. Moreover, the integration of formal elements in the language makes it more precise and facilitates the development of automated tools for processing the graphical models.

9 APPENDICES

The following appendices are to be found in separate documents.

A. Legal Risk Analysis of CE Scenario with Respect to IPR

B. Analysis of International Issues with Respect to the AS Scenario

C. Analysis of Data Protection Law

D. Conceptual Model for Legal Risk Analysis

E. User-level Language for the Analysis of Legal Risks